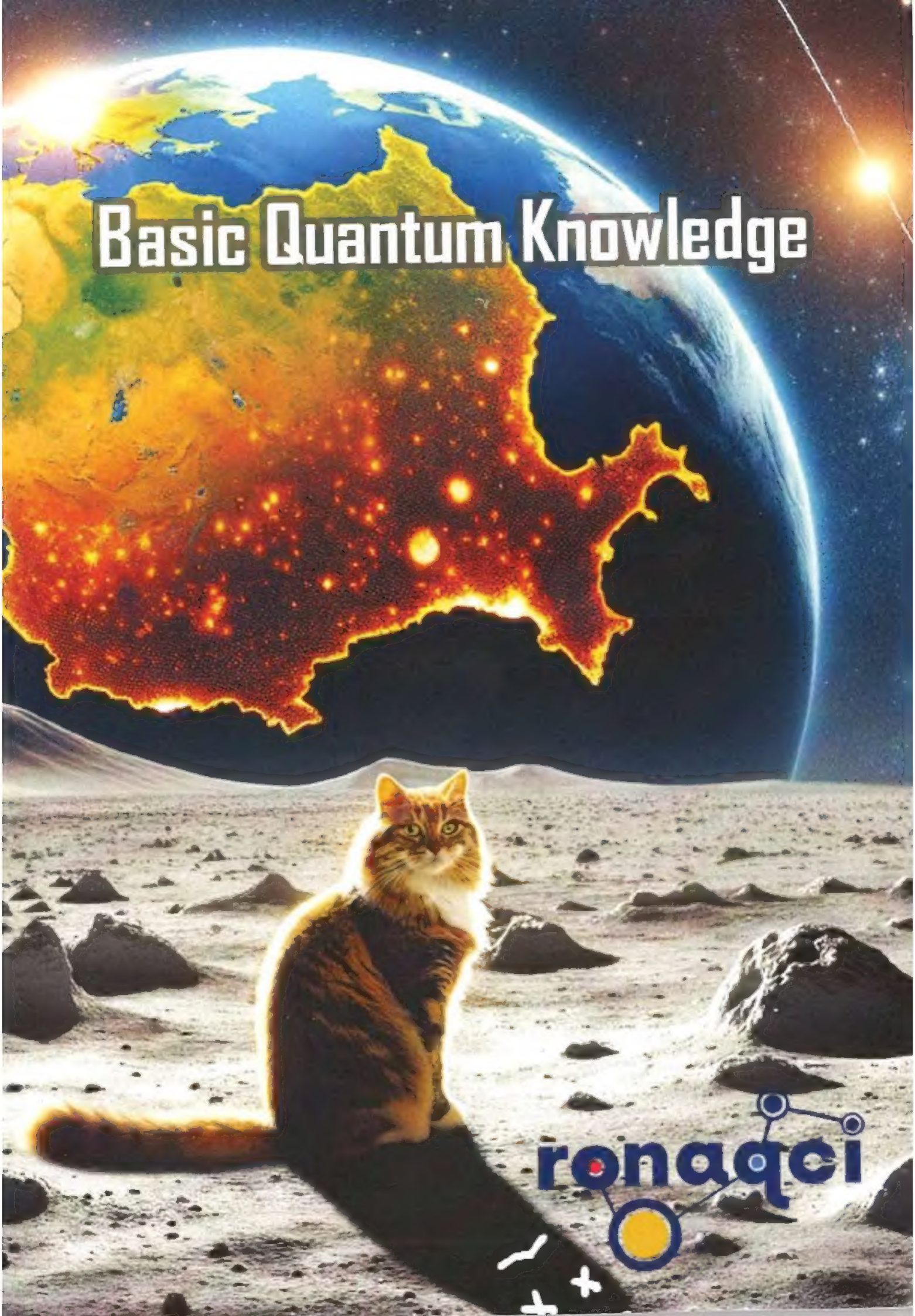
Basic Quantum Knowledge



ronaqci

BASIC QUANTUM KNOWLEDGE

basic
QUANTUM
knowledge

Editura POLITEHNICA PRESS
BUCUREȘTI, 2024

Adresă: Calea Griviţei, 132
10737, Sector 1, Bucureşti
Telefon: 021.402.90.74

Descrierea CIP a Bibliotecii Naţionale a României
Basic Quantum knowledge. - Bucureşti : Politehnica Press, 2024
Conţine bibliografie
ISBN 978-606-9608-88-3

53

Foreword

This manuscript was developed in order to respond to the necessity of the Romanian educational system to bring quantum knowledge closer to the community, leading to a concrete involvement into the new emerging quantum reality.

Most universities and research institutes from Romania decided in 2023 to create a large research and educational consortium of Quantum Hubs (18 and counting), geographically spread in cities like Bucharest, Cluj, Iaşi, Timişoara, Constanţa, Sibiu and Craiova. An important intention of this consortium is to create a large number of trained users in quantum technologies and part of this intention is funded by the *RoNaQCI: Romanian National Quantum Communication Infrastructure*[1] project, belonging to *EuroQCI*.

The starting point for this continuous process of training is this manuscript that provides a good introduction to basic quantum knowledge (it includes topics like *single qubit gates, measurement, systems with multiple qubits, universal gates, no-cloning theorem, superdense coding protocol, entanglement, teleportation, BB84, quantum key distribution*, etc.) and brings together all the necessary prerequisites (algebra and physics) in the first part, entitled *From previous episodes*. We mention here three of the most important manuscripts that have guided the content of this initiative, i.e. [1, 2, 3].

In the process of writing this manuscript[2], the following partners with established experience in teaching quantum knowledge, were involved: *National University of Science and Technology POLITEHNICA Bucharest (as coordinator), "Gheorghe Asachi" Technical University of Iaşi, Technical University of Cluj-Napoca, Western University of Timişoara, "Alexandru Ioan Cuza" University of Iaşi, University of Bucharest, "Horia Hulubei" National Institute, National Institute for Research and Development of Isotopic and Molecular Technologies.*

Authors, June 2024

[1]This manuscript has been funded by RoNaQCI, part of EuroQCI, DIGITAL-2021-QCI-01-DEPLOY-NATIONAL, 101091562.

[2]The manuscript follows the structure of [4].

Contents

List of Figures

From Previous Episodes

Short course on Linear Algebra adapted for Quantum Computing

The goal of this course module[3] is to familiarize students with the terminology and the mathematical notation used in Quantum Mechanics (QM). Linear Algebra provides the mathematical foundation for formulating principles and other results in QM. In this regard, we will review fundamental concepts: vector spaces, linear transformations, abstract vectors, the relationship between linear transformations and matrices (through fixed bases), classes of matrices, etc.

Linear spaces over $\mathbb{C}$

In college, we have mainly studied vector spaces (also known as linear spaces) over $\mathbb{R}$. These spaces are well suited to describing geometry and dynamics. The coordinates are $\mathbf{x}, \mathbf{y}, \mathbf{z}$. A box of length x, width y, height z with one corner in the origin, would have the farthest corner at $\mathbf{r} = x \cdot \mathbf{x} + y \cdot \mathbf{y} + z \cdot \mathbf{z}$. In QM, we use different types of spaces to describe the quantum states. Our coordinates are a set of states chosen depending on the type of quantum system that is modeled, and our scalars belong to the space $\mathbb{C}$, rather than $\mathbb{R}$. The quantum objects have a dual character, wave and particle. To describe the wave aspect, one needs two real scalars, an amplitude and an angle. These scalars can be condensed into a single complex number.

A **complex linear space** (equivalent to over $\mathbb{C}$) is a set V, endowed with an addition operation $(u + v)$ and another operation of scalar multiplication (λu) with $u, v \in V, \lambda \in \mathbb{C}$, with well-known properties. Usually, we will use finite-dimensional complex linear spaces, having $\mathbb{C}^n$ as a prototype space $(n \geq 1)$. Any abstract vector $v \in \mathbb{C}^n$ is an ordered set (equivalent to array) of n complex numbers. We adopt the usual convention, in which v is written as an $n \times 1$ column matrix of the form:

[3]This chapter follows the content of [5].

$$v = \begin{pmatrix} v_0 \\ v_1 \\ \vdots \\ v_{n-1} \end{pmatrix}$$

The j-th element is denoted by v_j. With transparent notation, the opposite $-v$, the conjugate $\overline{v}$ (also denoted as v^*), the transpose v^{T}, the sum $v + v'$, and the scalar multiple λv are defined, with the usual computational properties.

Definition 1. *(Dirac's Convention): If v represents the state of a system, then it is denoted as $|v\rangle$ and called a ket-vector. It is associated with the bra-vector $\langle v| = (\overline{v})^{\mathsf{T}} \equiv (v^{\mathsf{T}})^*$ (also referred to as the dual or dagger ($\equiv \dagger$) of v). The null vector in $\mathbb{C}^n$ is denoted as 0, not $|0\rangle$ or $\langle 0|$.*

Examples:

I Let the vector v be in $\mathbb{C}^2$ with components $2+3i$ and -1. Then

$$|v\rangle = \begin{pmatrix} 2+3i \\ -1 \end{pmatrix} \text{ and } \langle v| = \begin{pmatrix} 2-3i, & -1 \end{pmatrix} = v^\dagger \text{ (conjugate transpose } v\text{)}.$$

II If

$$|v\rangle = \begin{pmatrix} 1-i \\ 2+3i \\ 3 \\ -i \end{pmatrix} \text{ then } v^\dagger = \langle v| = \begin{pmatrix} 1+i, & 2-3i, & 3, & i \end{pmatrix}.$$

III If $e_0 = (1, 0, \ldots, 0) \in \mathbb{C}^n$, then

$$|e_0\rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \text{ and } \langle e_0| = \begin{pmatrix} 1, & 0, \ldots, & 0 \end{pmatrix}$$

and more generally, if $v = (v_0, v_1, \ldots, v_{n-1})$, then $\langle v| = (\overline{v_0}, \overline{v_1}, \ldots, \overline{v_{n-1}})$.

IV The space $\mathbb{C}^n$ is isomorphic to $\mathbb{R}^{2n}$, and for $n \geq 2$, the elements of $\mathbb{C}^n$ cannot be visualized (the human brain is not equipped for it!); however, algebraic manipulations and forced geometric interpretations can be used.

If V is a complex linear space and $S = \{|v_1\rangle, \ldots, |v_p\rangle\}$ is a system of vectors, we recall that S **generates** V (equivalently, it is a **set of generators**) if any vector $|v\rangle \in V$ is a linear combination of vectors from S ($|v\rangle = \sum_k a_k |v_k\rangle$); then S is **linearly independent** if from the relation $\sum_k a_k |v_k\rangle = 0$, it follows that all the complex coefficients a_k are zero.

If S is both a set of generators and linearly independent, it is a **basis** of V. The space V can have multiple distinct bases (even infinitely many), but they all have the same number of elements, called the **dimension** of V.

We'd like to remind that any linearly independent system in V can be completed by adding new vectors to form a basis for V; furthermore, from any set of generators, some can be removed until obtaining a basis.

We also emphasize that an application $A : V \to W$ between two complex linear spaces is called **linear** if $A\left(\sum_k a_k|v_k\rangle\right) = \sum_k a_k A\left(|v_k\rangle\right) \equiv \sum_k a_k A|v_k\rangle$ [We will write $A|v\rangle$ instead of $A\left(|v\rangle\right)$].

A **linear operator** on the space V is a linear application $A : V \to V$.

Examples:

I The **zero operator** $0 \equiv 0_V$ associates the zero vector with any vector $|v\rangle$. The **identity operator** $I = I_V$ associates any vector $|v\rangle$ with itself.

II If $A : V \to W$ is a linear application defined only on the vectors of a basis of V, then it extends to the entire space V.

III If $A : V \to W$ and $B : W \to Z$ are linear applications, then the composition $B \circ A$ (also denoted as BA) is also linear: $(BA)\,|v\rangle = B\left(A\,v\rangle\right)$.

For any matrix $A \in M_{m,n}(\mathbb{C})$, the following can be associated: **transpose** A^T, **conjugate** $\bar{A} = A^*$, and **dagger** $A^\dagger \equiv \left(A^*\right)^\mathsf{T} = \left(A^\mathsf{T}\right)^*$, which is the transpose of the conjugate. Of course, $(AB)^\mathsf{T} = B^\mathsf{T}A^\mathsf{T}$, $(AB)^* = A^*B^*$, $(AB)^\dagger = B^\dagger A^\dagger$. $\left(A^\mathsf{T}\right)^\mathsf{T} = A$, $(A^*)^* = A$, $\left(A^\dagger\right)^\dagger = A$. If $A \in M_{m,n}(\mathbb{C})$, then $A = (a[i,j])$; $0 \leq i \leq m-1$, $0 \leq j \leq n-1$. Then $A^\dagger[j,k] = A[k,j]^*$.

Examples:

I If

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \text{ then } A^\dagger = \begin{pmatrix} a^* & c^* \\ b^* & d^* \end{pmatrix}.$$

II If $A \in M_{m,n}(\mathbb{C})$ and $v \in \mathbb{C}^n$, the matrix product $A \cdot |v\rangle$ is also denoted as $A|v\rangle$. Therefore, if

$$A = \begin{pmatrix} 2 & i \\ 1 & 0 \\ i & -2 \end{pmatrix} \text{ and } v = \begin{pmatrix} 1-i \\ 0 \end{pmatrix}, \text{ then } A|v\rangle = \begin{pmatrix} 2 & i \\ 1 & 0 \\ i & -2 \end{pmatrix} \cdot \begin{pmatrix} 1-i \\ 0 \end{pmatrix} = \begin{pmatrix} 2-2i \\ 1 \\ 1+i \end{pmatrix}.$$

Abstract Vector Inner Products, Orthonormal Bases

Let V be a complex linear space.

Definition 2. *To define an* ***inner product (IP)*** *in V means to associate a complex scalar to any two vectors $v, u \in V$, denoted as $\langle v|w\rangle$ (or (v,w)), with the following properties:*

IP1. $\langle v|v\rangle$ is a real number ≥ 0, which is zero $\rightleftharpoons v = 0$;
IP2. $\langle v|w\rangle = \langle w|v\rangle^*$ for any $v, w \in \mathbb{C}^n$; in particular, $\langle v|v\rangle$ is a real number ≥ 0;
IP3. Linearity with respect to the second argument, i.e., $\langle v|w + w'\rangle = \langle v|w\rangle + \langle v|w'\rangle$ and $\langle v|\alpha\, w\rangle = \alpha\langle v|w\rangle$ for any scalar $\alpha \in \mathbb{C}$.

The norm of a vector $v \in V$ is the real non-negative number $||v|| = \langle v|v\rangle^{\frac{1}{2}}$.

It is said that V is endowed with an IP (inner product).

Examples:

1. IP euclidian ($\equiv$ standard) in space $V = \mathbb{C}^n$ is: if $a = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$ and $b = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$,

   the matrix product is defined as

$$\langle a, b\rangle = a^\dagger \cdot |b\rangle = (a_1^*, \ldots, a_n^*) \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = a_1^*\, b_1 + \cdots + a_n^*\, b_n. \tag{0.1}$$

   The properties IP1 - IP3 are easily verified. The Euclidean norm of $a = a\rangle$ is

$$||a|| = \langle a, b\rangle^{\frac{1}{2}} = \left(a^\dagger \cdot |b\rangle\right)^{\frac{1}{2}} = \left(|a_1|^2 + \cdots + |a_n|^2\right)^{\frac{1}{2}}. \tag{0.2}$$

   The normalized (equiv. versor) of a nonzero vector a is $\frac{1}{|a|}a$.

   Therefore, the Euclidean scalar product

$$\langle a, b\rangle = \text{matrix product (bra a)} \cdot \text{(ket b)} = a^\dagger \cdot |b\rangle,$$

   which justifies the terminology proposed by Dirac.

2. If $A \in M_{m,n}(\mathbb{C})$ and v, w are column vectors, IP $\langle v|A \cdot w\rangle$ can be noted as $\langle v|A|w\rangle$. Therefore, $\langle v|A\, w\rangle = v^* \cdot (A \cdot w) = (v^* \cdot A) \cdot w = \langle A^\dagger \cdot v|w\rangle$.

3. Let us consider $V = L^2_{\mathbb{R}}$ the complex linear space of functions $\psi : \mathbb{R} \to \mathbb{C}$ that are square-integrable (i.e., $\int_{\mathbb{R}} |\psi(t)|^2\, \mathrm{d}t < \infty$); For example $\psi(t) = exp(-t^2)$ belongs to $V = L^2_{\mathbb{R}}$. The space V is infinite-dimensional, but it can be endowed with an inner product (IP) by defining $\langle \varphi|\psi\rangle = \int_{\mathbb{R}} \varphi^*(t) \cdot \psi(t)\, \mathrm{d}t$. The vectors $\psi \in V$ are called **kets** and are denoted as $|\psi\rangle$. Continuous linear functionals from $V \to \mathbb{C}$ are called **bras** and their set is denoted as V' (**the dual** of V).

For any ket $\varphi \in V$, one can define the bra $\omega_\varphi : V \to \mathbb{C}$ as $\upsilon \mapsto \langle \varphi|\upsilon\rangle$, while Riesz's theorem shows that the mapping $V \to V'$, $\varphi \mapsto \omega_\varphi$, is an isomorphism. There exists a bijective correspondence between bras and kets.

Definition 3. *Let V be a linear space endowed with an inner product (IP). Two vectors $v, w \in V$ are called* ***orthogonal*** *if $\langle v|w\rangle = 0$. A system of vectors $\{v_1, \ldots, v_p\}$ in V is called* ***orthonormal*** *if $\langle v_i|v_j\rangle = \delta_{ij}$ for $1 \leq i, j \leq p$.*

In particular, for any i, $||v_i|| = 1$, so v_i is a versor. It is easily shown that any orthonormal system is linearly independent (but not vice versa).

Question: What does it mean that $dim\, V = n$?

Answer: In the space V, there exists a basis, which is a system of exactly n vectors, that are generators and linearly independent. For example, $dim\, V = 1$ if V has at least one nonzero vector. If the vectors v_1 and v_2 in V are linearly independent, then $dim\, V \geq 2$, and you can add $n-2$ more vectors to obtain a basis for V. Additionally, a basis in V is a basis in the usual sense.

Definition 4. *Let V be a (complex) linear space endowed with an inner product (IP), of dimension n. An* ***orthonormal basis*** *of V (abbreviated as b. o.) is a system of n orthonormal vectors.*

Not every basis of V is orthonormal. In the space $\mathbb{C}^n$, there are infinitely many orthonormal bases.

Examples:

1. To any quantum system with a finite number of basis states is associated a Hilbert space ($\equiv$ a finite-dimensional complex linear space V, endowed with an IP). Thus, a qubit is associated with a Hilbert space V of dimension 2, with the basis states symbolically denoted as $|0\rangle$ and $|1\rangle$, forming an orthonormal basis.

2. The computational basis of $\mathbb{C}^2$ is $B = \{e_0, e_1\}$, where $e_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$ and $e_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$. Relative to the Euclidean IP, this is an orthonormal basis because $\langle e_i, e_j\rangle = \delta_{ij}$ for any i, j. Similarly, the computational basis of $\mathbb{C}^3$ is $\{e_0, e_1, e_2\}$, where

$$e_0 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \; e_1 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \text{and } e_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

The Hadamard Basis of $\mathbb{C}^2$ is $B_H = \{h_1, h_2\}$, where $h_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{e_0 + e_1}{\sqrt{2}}$, $h_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{e_0 - e_1}{\sqrt{2}}$, and it is obviously an orthonormal basis.

We have seen that the polarization of light is achieved through specialized filters. We denote by $f_1 = |\uparrow\rangle$ and by $f_2 = |\rightarrow\rangle$ the vertical and horizontal polarization versors, respectively. The polarization state of a photon is realized through a polarization versor $|v\rangle$: f_1 and f_2 form an orthonormal basis over the linear space $\mathbb{R}^2/\mathbb{R}$ (just like for $\mathbb{C}^2/\mathbb{C}$), and $|v\rangle$ is uniquely written as

$$|v\rangle = a|\uparrow\rangle + b|\rightarrow\rangle, \text{with } |a|^2 + |b|^2 = 1.$$

Definition 5. *If V and W are two linear spaces endowed with inner products, then for any fixed vectors $v \in V$ and $w \in W$, we can define the linear map*

$$f : V \to W, \quad f(u) = \langle v|u\rangle w, \tag{0.3}$$

called the ***outer product*** *of the vectors v and w, denoted as $|w\rangle\langle v|$.*

Some Applications:

Let V be a complex linear space endowed with an orthonormal basis $B = \{e_i\} \equiv \{|i\rangle\}$.

a) **Expression of the Inner Product relative to the B basis**

Let v and w be any two vectors in V, so $v = \sum_i v_i e_i$, $w = \sum_i w_i e_i$. Then

$$\langle v|w\rangle = \langle \sum_i v_i e_i | \sum_j w_j e_j \rangle = \sum_{i,j} \overline{v_i} w_j \langle e_i|e_j\rangle = \sum_{i,j} \overline{v_i} w_j \delta_{ij} = \sum_i \overline{v_i} w_i,$$

that is, precisely the Euclidean inner product, as per (0.1), of the components ($\equiv$ coordinates) of v and w relative to the same basis.

b) **The completeness relation**

Any vector u in V can be uniquely written as $u = \sum_i u_i e_i$, so $\langle e_i|u\rangle = \langle e_i| \sum_k u_k e_k\rangle = \sum_k u_k \langle e_i|e_k\rangle = \sum_k u_k \delta_{ik} = u_i$, for any i.

The projection operator onto the direction of the unit vector e_i can also be defined as follows:

$$p_i : V \to V, \; u \mapsto u_i e_i = \langle e_i|u\rangle e_i \tag{0.4}$$

Therefore, $p_i(u) = \langle e_i|u\rangle e_i = |e_i\rangle\langle e_i|(u)$, (0.3), for any i $(1 \leq i \leq n)$, that means $p_i = |e_i\rangle\langle e_i|$.

Let $I = I_V : V \to V$ be the identity operator ($I(v) = v$ for any $v \in V$). Then, for any $u \in V$, we have $\sum_i p_i(u) = \sum_i u_i e_i = u = I_V(u)$, as shown in Equation (0.4). In conclusion,

$$\sum_i p_i = I_V \text{ or } I_V = \sum_i |e_i\rangle\langle e_i|. \tag{0.5}$$

The equation (0.5) is called the **completeness relation** (or **resolution / decomposition of the identity**).

c) **Connection between Linear Transformations and Matrices**

Let V and W be two finite-dimensional complex linear spaces endowed with inner products, and let $A : V \to W$ be a linear transformation. We fix a basis $B = \{v_j\}$ in V and $B' = \{w_i\}$ in W. Then, for any j, we have $A(v_j) = \sum_i a_{ij} w_i$, where $a_{ij} = \langle A(v_j)|w_i\rangle$.

Definition 6. *The matrix $\mathcal{A} = (a_{ij})$ is called the* ***matrix associated with the transformation*** *A* ***with respect to the bases*** *B and B' (denoted as $M_A^{B,B'}$), or the* ***matrix representation*** *of the transformation A. In the case of a linear operator $A : V \to V$ and choosing $B' = B$, the matrix $\mathcal{A}$ is square (denoted as M_A^B and not $M_A^{B,B}$).*

Examples:

1. Let $V = \mathbb{C}^2$ with the Euclidean inner product space, and $B = \{e_0, e_1\}$ be the basis. The matrix associated with the operator $A : V \to V$, $e_0 \mapsto e_1$, $e_1 \mapsto e_0$ is $\mathcal{A} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. The matrix associated with the zero operator is the zero matrix, and if $A = I_V$, then $\mathcal{A}$ is the identity matrix I_n (where $n = dim V$).

2. If $\mathcal{A} = (a_{ij})$ is a matrix in $M_{m,n}(\mathbb{C})$, it is associated with the linear transformation
$$A : \mathbb{C}^n \to \mathbb{C}^m, \ |v\rangle \mapsto \mathcal{A}|v\rangle.$$
The matrix associated with A relative to the computational bases and Euclidean inner product space is precisely $\mathcal{A}$.

We write $A = I_W \circ A \circ I_V$ (composition of linear transformations). According to (0.5), we have $I_W = \sum_i |w_i\rangle\langle w_i|$ and $I_V = \sum_j |v_j\rangle\langle v_j|$ so $A = \left(\sum_i |w_i\rangle\langle w_i|\right) \circ A \circ \left(\sum_j |v_j\rangle\langle v_j|\right) = \sum_{i,j} |w_i\rangle \left(\langle w_i|A|v_j\rangle\right) \langle v_j|$. However, $\langle w_i|A|v_j\rangle$ is precisely equal to the element a_{ij} of the matrix $\mathcal{A}$, and we obtain the relationship

$$A = \sum_{i,j} a_{ij} |w_i\rangle\langle v_j|, \tag{0.6}$$

called the **representation of operator A using the outer product.**

Note: The connection between linear transformations (A) and matrices ($\mathcal{A}$) is very tight but non-canonical in the sense that it depends on the choice/fixing of bases.

Basis change. Eigenvectors and eigenvalues

Given two distinct bases in $\mathbb{C}^n$, an important question is how to relate the representations of the same vector in the two bases. This problem is central in physics since the same physical quantity may be represented in different reference frames and one is interested in the relations between these various representations such that universal properties of the physical quantity become salient.

Let $B = \{e_i\}$ be an orthonormal basis in $\mathbb{C}^n$. Any vector $x \in \mathbb{C}^n$ can be uniquely written as $x = \sum_i x_i e_i$, and

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

represents the column vector of coordinates of x relative to the basis B. If $B' = \{e'_i\}$ is another orthonormal basis in $\mathbb{C}^n$, and X' is the column vector of coordinates of x relative to the basis B', we aim to establish the relationship between X and X'. We have $e'_j = \sum_i t_{ij} e_i$ for any j, $1 \leq j \leq n$.

Definition 7. *The matrix $T_{B\to B'} = (t_{ij})$, a square matrix of order n, is called the* ***transition matrix from basis B to basis B'.***

We have $x = \sum_i x_i e_i = \sum_j x'_j e'_j = \sum_j x'_j \left(\sum_i t_{ij} e_i\right) = \sum_i \left(\sum_j t_{ij} x'_j\right) e_i$; therefore, $\sum_i \left(x_i - \sum_j t_{ij} x'_j\right) e_i = 0$. Since the vectors e_i are linearly independent, it follows that $x_i = \sum_j t_{ij} x'_j$ for every i. These relationships can be compactly expressed in matrix form. Specifically,

Proposition 1. *We have*

$$X = T_{B\to B'} \cdot X'. \tag{0.7}$$

This is the desired relationship. Symmetrically, $X' = T_{B'\to B} \cdot X$, so $X = T_{B\to B'} \cdot T_{B'\to B} \cdot X$. Since X is an arbitrary column matrix, it follows that $T_{B\to B'} \cdot T_{B'\to B} = I_n$.

COROLLARY. Any transition matrix $T_{B\to B'}$ is nonsingular, and its inverse is precisely the matrix $T_{B'\to B}$.

Examples:

1. Let the bases be $B = \{e_1, e_2\}$ with $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, forming the computational basis in $\mathbb{C}^2$. Additionally, consider the Hadamard basis $B_H = \{h_1, h_2\}$ with $h_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, $h_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$, both forming an orthonormal basis. The transition matrix from B to B_H is

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

and its inverse is denoted as $H^{-1} \equiv H^{\mathsf{T}}$.

If $q \in \mathbb{C}^2$, $q = \begin{pmatrix} a \\ b \end{pmatrix} = ae_1 + be_2$ it is also stated as follows: qubit q is the **superposition** of the base qubits e_1, e_2. However, $\begin{pmatrix} e_1 \\ e_2 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} h_1 \\ h_2 \end{pmatrix}$, so $e_1 = \frac{1}{\sqrt{2}}(h_1 + h_2)$, $e_2 = \frac{1}{\sqrt{2}}(h_1 - h_2)$, and $q = a\frac{1}{\sqrt{2}}(h_1 + h_2) + b\frac{1}{\sqrt{2}}(h_1 - h_2) = \frac{a+b}{\sqrt{2}} h_1 + \frac{a-b}{\sqrt{2}} h_2$. Therefore:

The **superposition** of qubits depends on the chosen basis.

Note: Formula (0.7) extends the rotation formulae (in $\mathbb{R}^2, \mathbb{R}^3$) of reference frames from analytic geometry. For example, the position of an artificial satellite ("point-like") of the Moon is determined in relation to a frame of reference on the Moon and the position of the same satellite relative to a frame of reference on Earth are linked by relationships of type (0.7).

Let there be a linear operator $f : \mathbb{C}^n \to \mathbb{C}^n$ and $B = \{v_i\}$ a basis of $\mathbb{C}^n$. For any j, $f(v_j) = \sum_i a_{ij} v_i$.

Definition 8. *The matrix $M_f^B = (a_{ij})$, $1 \leq i, j \leq n$ is called the* ***matrix of the operator f relative to the basis B.***

Let $x \in \mathbb{C}^n$ be an **arbitrary** vector, and $y = f(x)$. We have $x = \sum_j x_j v_j$ and $y = \sum_i y_i v_i$. Denoting $X = (x_1, \ldots, x_n)^T$ and $Y = (y_1, \ldots, y_n)^T$ as the coordinate vectors of x and $y = f(x)$ relative to basis B, we get the relation

$$Y = M_f^B \cdot X. \tag{0.8}$$

If $B' = \{v_i'\}$ is another basis of $\mathbb{C}^n$, X' is the matrix of coordinates of x relative to B', and Y' is the matrix of coordinates of $f(x)$ relative to B', then $Y' = M_f^{B'} \cdot X'$, according to (0.8). Denoting $T = M_{B \to B'}$ as the transition matrix from basis B to B', the relation (0.7) shows that $X = T \cdot X'$ and $Y = T \cdot Y'$. Therefore, according to (0.8), $M_f^B \cdot X = T \cdot M_f^{B'} \cdot X'$, which implies $M_f^B \cdot T \cdot X' = T \cdot M_f^{B'} \cdot X'$. Since the vector X' is arbitrary, we obtain the relation $M_f^B \cdot T = T \cdot M_f^{B'}$. Because the matrix T is nonsingular, it follows that

$$M_f^{B'} = T^{-1} \cdot M_f^B \cdot T. \tag{0.9}$$

We recall that two square matrices A, A' of the same order n are **similar** if there is a nonsingular matrix T of order n such that $A' = T^{-1}AT$. Therefore, we showed

Proposition 2. ***The matrices of an operator*** *$f : \mathbb{C}^n \to \mathbb{C}^n$ with respect to two bases B, B' (not necessarily orthonormal) of the space $\mathbb{C}^n$ are similar.*

Definition 9. *Let V be a complex linear space of dimension n (in particular, $V = \mathbb{C}^n$), and $f : V \to V$ be a linear operator. A scalar $\lambda \in \mathbb{C}$ is called an* ***eigenvalue of f if there exists a nonzero vector v such that***

$$f(v) = \lambda v, \text{ meaning } (f - \lambda 1_V)(v) = 0. \tag{0.10}$$

A vector $v \in V$ is called an **eigenvector of f** if $v \neq 0$ and there exists $\lambda \in \mathbb{C}$ such that $f(v) = \lambda v$.

If $A \in M_n(\mathbb{C})$ is a square matrix, any number $\lambda \in \mathbb{C}$ is called an **eigenvalue of A** if there exists a nonzero column vector v (a $n \times 1$ matrix) such that $A\lambda = \lambda v$, meaning $(A - \lambda I_n)v = 0$. An **eigenvector** for A is a nonzero column vector v such that there exists $\lambda \in \mathbb{C}$ and $Av = \lambda v$.

Let B be a basis of the space $\mathbb{C}^n$, and $f : V \to V$ be a linear operator. Denoting $A = M_f^B$, the matrix of the operator f with respect to the basis B (Definition 8), it follows that the eigenvalues and eigenvectors of f are the same as those of the matrix A. A complex number $\lambda \in \mathbb{C}$ is an eigenvalue if there exists a nonzero column vector v (an $n \times 1$ matrix) such that $(A - \lambda I_n)v = 0$. This relation is, in fact, a linear homogeneous system with n equations and n unknowns, having a nonzero solution v, so necessarily, $\det(A - \lambda I_n) = 0$.

Definition 10. *The polynomial of degree n*

$$P_A(X) = \det(A - XI_n) \tag{0.11}$$

is called ***the characteristic polynomial*** *of matrix A.*

If B' is another basis in $\mathbb{C}^n$ and $C = M_f^{B'}$, we saw (Proposition 2) that matrix A and C are similar, i.e., there is nonsingular $T \in M_n(\mathbb{C})$ such that $C = T^{-1}AT$. Then $P_C(X) = \det(C - XI_n) = P_A(X)$, and the polynomial $P_A(X)$ is independent of basis B (for which $A = M_f^B$), i.e., it is associated to operator f, and, therefore, denoted $P_f(X)$.

We recall the fundamental theorem (Gauss-d'Alembert) of algebra: "Any polynomial $P \in \mathbb{C}[X]$ of degree $n \geq 1$ has at least a complex root". It follows that $\lambda_1, \ldots, \lambda_p$ are distinct roots of P, with multiplicities $n_1, \ldots, n_p \geq 1$, then $P(X) = a_0(X - \lambda_1)^{n_1} \ldots (X - \lambda_p)^{n_p}$, with $n_1 + \cdots + n_p = n$.

Definition 11. *Given a linear operator $f : V \to V$, we consider the characteristic polynomial, using a basis B and the matrix $A = M_f^B$.* ***The spectrum of the operator*** *f is the set*

$$Spec\, f = \begin{Bmatrix} n_1, & \ldots, & n_p \\ \lambda_1, & \ldots, & \lambda_p \end{Bmatrix},$$

of distinct eigenvalues λ_j, $j = 1, 2, 3, \ldots, p$, with their multiplicities n_j, $j = 1, 2, 3, \ldots, p$.

Therefore, $P_f(\lambda) = (-1)^n \cdot (\lambda - \lambda_1)^{n_1} \ldots (\lambda - \lambda_p)^{n_p}$, with $n_1 + \cdots + n_p = n$.

Example: For $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, we have $P_A(\lambda) = \begin{vmatrix} -\lambda & 1 \\ 1 & -\lambda \end{vmatrix} = \lambda^2 - 1$, meaning $Spec\, A = \begin{Bmatrix} 1, & -1 \\ 1, & -1 \end{Bmatrix}$. For $\lambda = 1$, the eigenvectors are $v = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$ such that $Av = v$ and, therefore, $v = \begin{pmatrix} \alpha \\ \alpha \end{pmatrix}$, $\alpha \neq 0$. For $\lambda = -1$, the eigenvectors are $\begin{pmatrix} \beta \\ -\beta \end{pmatrix}$ with $\beta \neq 0$.

For any eigenvalue $\lambda \in Spec\, f$, one can consider the corresponding **eigensubspace** $V(\lambda) = \{v \in \mathbb{C}^n | f(v) = \lambda v\}$. Thus, eigenvectors with eigenvalue λ form $V_\lambda \setminus \{0\}$. It can be shown that $V(\lambda)$ is a linear subspace of V and $dim\, V(\lambda) \leq n_\lambda$.

Definition 12. *The operator f is called* ***diagonalizable*** *if there is a basis B of V such that the matrix M_f^B is diagonal. It is shown that f is diagonalizable $\Leftrightarrow$ $dim\, V(\lambda) = n_\lambda$ for any $\lambda \in Spec\, f$, in which case the following decomposition in a direct sum of subspaces holds: $V = V(\lambda_1) \bigoplus \cdots \bigoplus V(\lambda_p)$.*

For any $x \in V$, we have the decomposition $x = \sum_i x_i$ with $x_i \in V(\lambda_i)$ so $f(x) = \sum_i f(x_i) = \sum_i \lambda_i x_i$. Considering the projection operator $p_i : V \to V(\lambda_i)$, $x \mapsto x_i$; then $\forall x \in V$, $f(x) = \sum_i \lambda_i p_i(x)$, i.e.,

$$f = \sum_i \lambda_i p_i \text{ and, } p_i = |i\rangle\langle i|. \tag{0.12}$$

Equation (0.12) is also called the "spectral theorem".
All the applications may be reformulated for matrices and not only for operators.

Examples:

1. Let us consider the Pauli matrix $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. The two eigenvalues are $\lambda_1 = 1$ and $\lambda_2 = -1$. We have $V(\lambda_1) = \{\begin{pmatrix} a \\ 0 \end{pmatrix} | a \neq 0\}$ and $V(\lambda_2) = \{\begin{pmatrix} 0 \\ b \end{pmatrix} | b \neq 0\}$. Therefore, Z is diagonalizable (and already diagonal) According to (0.12), $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$.
   The matrix $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ is not diagonalizable.

2. If all the eigenvalues of f are simple (i.e., $\forall \lambda \in Spec\ f. n_\lambda = 1$), then the operator f is diagonalizable.

3. Let V be a linear space endowed with an inner product, and $dim\, V = d$. If W is a linear subspace of V of dimension k ($k < d$), then any basis $\{e_1, \ldots, e_k\}$ of W can be extended to a basis $B = \{e_1, \ldots, e_k, e_{k-1}, \ldots, e_d\}$ of V. The linear transformation
$$P : V \to V,\ x = \sum_{i=1}^{d} x_i e_i \mapsto \sum_{i=1}^{k} x_i e_i$$
is called the **projector** onto W. The relationship $P^2 = P$ holds, and the eigenvalues of P are 0 and 1.

Hermitian and unitary matrices

Definition 13. *A square matrix $A \in M_n(\mathbb{C})$ is called* ***Hermitian*** *if*

$$A^\dagger = A \text{ or equivalently, } A^\intercal = \overline{A}. \tag{0.13}$$

Therefore, if $A = (a_{ij})$, $1 \leq i, j \leq n$, A is Hermitian $\Rightarrow a_{ij} = \overline{a_{ji}}$ for any i, j.

Examples:

1. The matrix $A = \begin{pmatrix} 4 & 3+i \\ 3-i & -2 \end{pmatrix}$ is Hermitian.

2. If $A = (a_{ij})$ is Hermitian, then $a_{ii} = \overline{a_{ii}}$ and, therefore, all diagonal elements of A are real.

3. If $A \in M_n(\mathbb{R})$, that is all its elements are real, then A is Hermitian $\rightleftharpoons A$ it is symmetric (i.e., $A^T = A$).

Proposition 3. *(Properties of Hermitian matrices).*

Let $A \in M_n(\mathbb{C})$ be a Hermitian matrix.

a). Relative to the Euclidian inner product ($\langle a|b\rangle = a^\dagger \cdot b$), the following relationship holds

$$\langle Av|w\rangle = \langle v|Aw\rangle, \tag{0.14}$$

for all $v, w \in \mathbb{C}^n$.

b). The eigenvalues of Hermitian matrix A are real.

c). If λ, λ' are distinct eigenvalues of A, then the corresponding eigenvectors are orthogonal.

Definition 14. *Let V be a complex linear space endowed with an inner product. A linear operator $f : V \to V$ is called* ***self-adjoint*** *(or equivalently, Hermitian) if*

$$\forall v, w \in V,\ \langle f(v)|w\rangle = \langle v|f(w)\rangle. \tag{0.15}$$

Examples:

1. If $A \in M_n(\mathbb{C})$ is a Hermitian matrix, then the linear operator $f : \mathbb{C}^n \to \mathbb{C}^n$, $f(v) = Av$ is self-adjoint, according to the relation (0.14).

2. It is easily shown that for any linear operator $f : V \to V$, there exists a unique linear operator $f^\dagger : V \to V$ such that $\forall v, w \in V$, $\langle v|f(w)\rangle = \langle f^\dagger(v)|w\rangle$, called the **adjoint** of f. Of course, f is self-adjoint $\rightleftharpoons f^\dagger = f$.

3. If f and $g : V \to V$ are self-adjoint operators that commute with each other ($f \circ g = g \circ f$), then the composition $g \circ f$ is self-adjoint; indeed, $\forall v, w \in V$, $\langle (g \circ f)(v)|w\rangle = \langle g(f(v))|w\rangle = \langle f(v)|g(w)\rangle = \langle v|f(g(w))\rangle = \langle v|g(f(w))\rangle = \langle v|(g \circ f)(w)\rangle$.

Note: It can be shown that **every self-adjoint operator is diagonalizable** (Definition 12). Therefore, if $Spec\, f = \{\lambda_1, \ldots, \lambda_p\}$, then the spectral theorem (0.12) holds, which means the decomposition $f = \sum_i \lambda_i p_i$, where f is decomposed into the projection operators onto the p directions of the eigenvectors, with eigenvalues being the eigenvalues of f. Such a decomposition resembles the decomposition of white light into the spectrum of fundamental colors.

In Quantum Mechanics, the following fact is also utilized: if f and g are self adjoint operators that commute with each other, then they are diagonalizable in the same basis B (i.e., M_f^B and M_g^B are diagonal matrices).

> We will see that in Quantum Mechanics, any physical observable is associated with a Hermitian matrix (or a self-adjoint operator).

Definition 15. *A square matrix $A \in M_n(\mathbb{C})$ is called* ***unitary*** *if the following relation holds:*

$$A \cdot A^\dagger = I_n, \tag{0.16}$$

meaning that A is invertible and $A^{-1} = A^\dagger$ (thus, $A^\dagger \cdot A = I_n$).

Examples:

1. The rotation matrix

$$A = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}, \alpha \in \mathbb{R}$$

is unitary, with eigenvalues $\cos\alpha \pm i\sin\alpha$, but it is not Hermitian.

2. The matrices

$$\sigma_0 = I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \sigma_x = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_3 = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_4 = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

called the **Pauli matrices**, are both unitary and Hermitian. The same is true for the matrix $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ of Hadamard.

Proposition 4. *(**Properties of unitary matrices**).*

Let $A \in M_n(\mathbb{C})$ be a unitary matrix.

a). A preserves the Euclidean inner product.

b). A preserves the Euclidean norm and the measurement of angles.

c). If v is a ket vector (i.e., a column vector from $\mathbb{C}^n$), then knowing the transform $v' = Av$, we can directly recover v.

d). The eigenvalues of A have absolute value 1.

In Figure 0.1 are represented diagrammatically the inclusion (or lack thereof) relationships between various classes of matrices in $M_n(\mathbb{C})$: H-Hermitian, I-invertible, U-unitary matrices. Matrix $A_1 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ belongs to $H \setminus I$, $A_2 = \begin{pmatrix} 4 & 1 \\ 2 & -1 \end{pmatrix}$ belongs to $I \setminus U$ and $I \setminus H$; then $X, Y, Z \in I \cap H$, and so on.

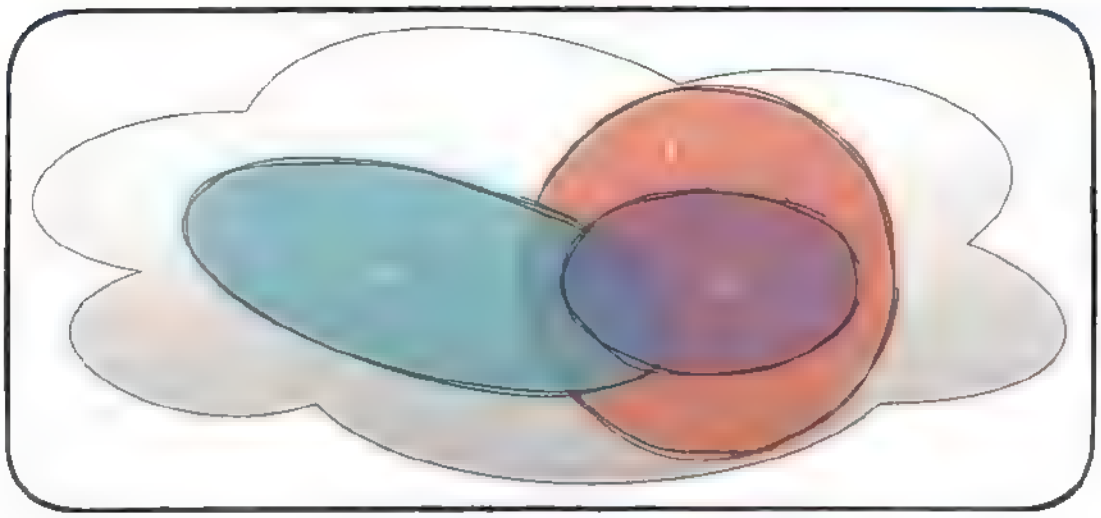


Fig. 0.1: The relationship between the Hermitian (H), Invertible (I), Unitary (U) classes of matrices.

Definition 16. *Let V be a (complex) linear space endowed with an inner product. A linear operator $f : V \to V$ is called* ***unitary*** *(or* ***isomorphism****) if, for any basis $B = \{e_i\}$ in V, $f(B) = \{f(e_i)\}$ is also a basis. Thus, unitary operators map bases to bases.*

Proposition 5. *(Properties of unitary operators).*

a). Unitary operators preserve inner products, norms, and distances.

b). The matrix of a unitary operator in a basis is unitary.

But also, if a linear operator $f : V \to V$ preserves inner products, then it is clearly unitary.

b) Let $f : V \to V$ be a unitary operator, B a basis, and $A = M_f^B = (a_{ij})$. Take arbitrary $x, y \in V$. We have $\langle f(x)|f(y)\rangle = \langle x|y\rangle$, so $\langle Ax|Ay\rangle = \langle x\, y\rangle$, i.e., $(AX)^\dagger \cdot AY = X^\dagger A^\dagger AY = X^\dagger Y$ (since $A^\dagger A = I_n$).

Note: In certain contexts, if A is a matrix and X is a column vector (such that the product AX makes sense), this product is called the result of the **action** of A on X. If A is unitary and $X' = AX$, then we have seen (Proposition 4 c)) that $X = A^\dagger X'$, so the action of A is canceled.

> In the quantum world, all actions (resulting from unitary operators) that are not measurements are reversible.

Unitary matrices with real coefficients ($A \cdot A^\mathsf{T} = I_n$) are called **orthogonal** (or **rotation matrices**). We will see that classical bits are processed through classical

logic gates, while qubits are processed through quantum logic gates described by unitary matrices.

We have presented several classes of matrices or linear operators: invertible, self-adjoint, unitary. There are also other types of operators studied in Functional Analysis. Thus, a linear operator $A : V \to V$ is called **normal** if $AA^\dagger = A^\dagger A$, meaning that A commutes with its adjoint.

Examples: Self-adjoint operators ($A^\dagger = A$) and unitary operators ($AA^\dagger = I_V$) are evidently normal.

The following holds:

Theorem (Spectral Decomposition). *"Let V be a finite-dimensional complex linear space equipped with an inner product. A linear operator $A : V \to V$ is normal if and only if A has a diagonal representation with respect to an orthonormal system $S = \{b_i\}$ of its eigenvectors, with eigenvalues λ_i, meaning that $A = \sum_i \lambda_i |e_i\rangle\langle e_i|$."*

We proved this theorem previously in the case of self-adjoint operators.

Furthermore, a linear operator $A : V \to V$ is called **positive** if $\forall v \in V$, the inner product $\langle v|Av\rangle$ is a real number ≥ 0. If, in addition, $\langle v|Av\rangle > 0$ for $v \neq 0$, then A is called **positive-definite**.

Example: For any A, the composite operator $A^\dagger \circ A$ is positive.

Tensor Products

Tensor product of two matrices

Definition 17. *For any two matrices $A = (a_{ij}) \in M_{m\,n}(\mathbb{C})$ and $B = (b_{ij}) \in M_{p,q}(\mathbb{C})$, their **tensor product** (or **Kronecker product**), denoted as $A \otimes B$, is defined as the following block matrix of size $mp \times nq$:*

$$A \otimes B = \left(\begin{array}{c|c|c|c} a_{11}B & a_{12}B & \dots & a_{1n}B \\ \hline a_{21}B & a_{22}B & \dots & a_{2n}B \\ \hline \vdots & \vdots & \vdots & \vdots \\ \hline a_{m1}B & a_{m2}B & \dots & a_{mn}B \end{array}\right) \tag{0.17}$$

In transparent notation, the following properties can be easily verified:

1. $(A_1 + A_2) \otimes B = A_1 \otimes B + A_2 \otimes B$; $\quad A \otimes (B_1 + B_2) = A \otimes B_1 + A \otimes B_2$;
2. $(\lambda A) \otimes B = \lambda (A \otimes B) = A \otimes (\lambda B)$; $\lambda \in \mathbb{C}$
3. $(A \otimes B) \otimes C = A \otimes (B \otimes C)$; dar $A \otimes B \neq B \otimes A$.
4. $(A \otimes B) \cdot (C \otimes D) = (A \cdot C) \otimes (B \cdot D)$, if the products $A \cdot C$ and $B \cdot D$ are defined; in particular, if v, v' are ket vectors ($\equiv$ columns), then $(A \otimes B)(v \otimes w) = (A \cdot v) \otimes (B \cdot w)$;
5. If A, B they are invertible square matrices, similarly, $A \otimes B$ is also invertible, and furthermore, $(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}$;

6. $(A \otimes B)^{\mathsf{T}} = A^{\mathsf{T}} \otimes B^{\mathsf{T}}$; $(A \otimes B)^{*} = A^{*} \otimes B^{*}$; $(A \otimes B)^{\dagger} = A^{\dagger} \otimes B^{\dagger}$;

7. If $\lambda_1, \lambda_2, \ldots, \lambda_n$ are the eigenvalues of $A \in M_n(\mathbb{C})$ (assuming distinct) and $\mu_1, \mu_2, \ldots \mu_m$ are the eigenvalues of $B \in M_m(\mathbb{C})$ (distinct), then the eigenvalues of $A \otimes B$ are the mn products $\lambda_i \mu_j$.

8. If $A \in M_n(\mathbb{C})$, $B \in M_m(\mathbb{C})$, then $\operatorname{tr}(A \otimes B) = \operatorname{tr}(A) \operatorname{tr}(B)$ and $\det(A \otimes B) = (\det A)^m (\det B)^n$.

Examples:

1. Let $A = \begin{pmatrix} 4 \\ 3 \end{pmatrix}$, $B = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $C = I_3$. Then $A \otimes B = \begin{pmatrix} 4B \\ 3B \end{pmatrix} = \begin{pmatrix} 4 \\ 0 \\ 3 \\ 0 \end{pmatrix}$,

$$B \otimes A = \begin{pmatrix} A \\ 0 \end{pmatrix} = \begin{pmatrix} 4 \\ 3 \\ 0 \\ 0 \end{pmatrix}, \quad A \otimes C = \begin{pmatrix} 4I_3 \\ 3I_3 \end{pmatrix} = \begin{pmatrix} 4 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \\ 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix} \text{ and } C \otimes A =$$

$$\left(\begin{array}{c|c|c} A & 0 & 0 \\ \hline 0 & A & 0 \\ \hline 0 & 0 & A \end{array}\right) = \begin{pmatrix} 4 & 0 & 0 \\ 3 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 4 \\ 0 & 0 & 3 \end{pmatrix}$$

2. If $e = \begin{pmatrix} 1 & 0 \end{pmatrix}$ and $e' = \begin{pmatrix} 0 & 1 \end{pmatrix}$ are 1×2 matrices, then $e \otimes e' = \left(\begin{array}{c|c} e' & 0 \end{array} \right) = \begin{pmatrix} 0 & 1 & 0 & 0 \end{pmatrix}$ and $e' \otimes e = \left(\begin{array}{c|c} 0 & e \end{array} \right) = \begin{pmatrix} 0 & 0 & 1 & 0 \end{pmatrix}$.

3. For the Pauli matrices, $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, we have

$$X \otimes Y = \begin{pmatrix} 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \\ 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \end{pmatrix} \text{ and}$$

$$I \otimes Z = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

4. If the square matrices A, B are Hermitian, then $A \otimes B$ is also Hermitian. Similarly, if A, B are unitary, then $A \otimes B$ is unitary as well.

5. Sometimes, a matrix M can be decomposed as the tensor product of two "smaller" matrices; in such cases, M is said to be separable. We will show that the ket vector $(4 \;\; 0 \;\; 0 \;\; 9)^{\mathsf{T}}$ cannot be decomposed in the form $v = \begin{pmatrix} x \\ y \end{pmatrix} \otimes \begin{pmatrix} a \\ b \end{pmatrix}$. Otherwise, it would imply that $xa = 4$, $xb = 0$, $ya = 0$, $yb = 9$ From the first equation, we have $a \neq 0$ which implies $y = 0$. However, this contradicts the equation $yb = 9$. But v can be decomposed as $v = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 4 \\ 0 \end{pmatrix} + (0 \;\; 3) \otimes (0 \;\; 3)$. In a similar manner,

$$\left(\begin{array}{cc|cc} 0 & 1 & 0 & -1 \\ 2 & 3 & -2 & -3 \\ \hline 0 & 0 & 0 & 2 \\ 0 & 0 & 4 & 6 \end{array}\right) = \begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix},$$

but the matrix

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}$$

cannot be decomposed.

> We will see that tensor products are used in assembling quantum systems and processing quantum states.

The tensor product of two linear spaces

Let V, W, Z be complex linear spaces, and $\beta : V \times W \to Z$ be a bilinear map ($\equiv$ being linear in each argument). In general, the imaginary

$$\operatorname{Im} \beta = \{\beta(v, w) \mid v \in V, w \in W\}$$

is not necessarily a linear subspace of Z.

Example: The multiplication operation $\beta : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$, defined as $\beta(v, w) = vw$ is bilinear, but it is not linear.

Definition 18. *The linear space Z is called a* ***tensor product*** *of the linear spaces V, W if there exists a bilinear map $\beta : V \times W \to Z$ such that the subspace generated by $\operatorname{Im} \beta$ in Z is exactly Z, and furthermore, for any bilinear map $\beta' : V \times W \to Z'$, there exists a linear map $f : Z \to Z'$ such that $f \circ \beta = \beta'$.*

The map f is unique (depending on β'), because if $g : Z \to Z'$ were another linear map such that $f \circ \beta = g \circ \beta$, then $\forall (v, w) \in V \times W$, we would have $f(\beta(v, w)) =$

$g(\beta(v, w))$. However, any element $z \in Z$ can be expressed as a linear combination of vectors of the form $\beta(v, w)$, so $f(z) = g(z)$, which means $g = f$.

In the context of the definition 18, the space Z is unique up to an isomorphism of linear spaces, and it is denoted as $V \otimes W$, so $\beta : V \times W \to V \otimes W$.

Definition 19. *For any $v \in V$, $w \in W$, it is denoted as*

$$v \otimes w = \beta(v, w) \tag{0.18}$$

called the ***tensor product*** *of the vectors v, w. The elements of $V \otimes W$ are called* ***tensors*** *and are finite linear combinations of products $v \otimes w$, because* $\operatorname{Im}\beta$ *generates $V \otimes W$ (i.e., it forms a system of generators).*

Examples:

1. Let $V = M_{2,1}(\mathbb{C}) \simeq \mathbb{C}^2$ and $W = M_{1,2}(\mathbb{C}) \simeq \mathbb{C}^2$. For $v = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$, $w = (b_1, b_2)$, $v \otimes w = \begin{pmatrix} a_1 w \\ a_2 w \end{pmatrix} = \begin{pmatrix} a_1 b_1 & a_1 b_2 \\ a_2 b_1 & a_2 b_2 \end{pmatrix}$ is defined in $M_2(\mathbb{C})$. The tensor product is isomorphic with $M_2(\mathbb{C})$. More general $M_{m,n}(\mathbb{C}) \otimes M_{p,q}(\mathbb{C}) \simeq M_{mp,nq}(\mathbb{C})$.

> Careful! $\mathbb{C}^2 \otimes \mathbb{C}^2 \simeq \mathbb{C}^4$; $\mathbb{C}^2 \otimes \mathbb{C}^3 \simeq \mathbb{C}^6$. But $\mathbb{C}^2 \otimes \mathbb{C}^3 \not\simeq \mathbb{C}^5$.

2. If $\{v_i\}$ forms an orthonormal basis in V and $\{v_i\}$ forms an orthonormal basis in W, then $\{v_i \otimes w_j\}$ forms a basis in $V \otimes W$.

Definition 20. *Let V, W, V', W' be complex linear spaces and $h : V \to W$, $h' : V' \to W'$, two linear maps. We can consider bilinear maps $\beta : V \times V' \to V \otimes V'$; $\beta^* : W \times W' \to W \otimes W'$; $(v, v') \mapsto h(v) \otimes h'(v')$*

Then there exists and is unique a linear map $F : V \times V' \to W \otimes W'$ so that $F \circ \beta = \beta^*$, named ***tensor product*** *of the maps h, h' and is denoted $h \otimes h'$: $F(v \otimes v') = h(v) \otimes h(v')$.*

Let V, W be finite dimensional, having the bases $B = \{v_1, \ldots, v_m\}$, $B' = \{w_1, \ldots, w_n\}$. It can be showed that the vectors $v_i \otimes w_j$ form a a basis for $V \otimes W$, denoted $B \otimes B'$. Therefore $\dim(V \otimes W) = \dim V \cdot \dim W$. The cartesian product $V \times W$ has the basis $\{(v_1, 0), \ldots, (v_m, 0), (0, w_1), \ldots, (0, w_n)\}$ and $\dim(V \times W) = \dim V + \dim W$.

Then, if $f : V \to V$ is a linear operator and $M = M_f^B$, and $g : W \to W$ is a linear operator having the matrix $N = M_g^{B'}$, then the matrix of $f \otimes g$ relative to the basis $B \otimes B'$ is $M \otimes N$, that is the Kronecker product 0.17.

The tensor product $v \otimes w$ of two state vectors is also noted with $|v\rangle \otimes |w\rangle \equiv |v\rangle|w\rangle$ or even $|vw\rangle$. We note that $\lambda(v \otimes w) = \lambda v \otimes w = v \otimes \lambda w$, $(v_1 + v_2) \otimes w = v_1 \otimes w + v_2 \otimes w$, $v \otimes (w_1 + w_2) = v \otimes w_1 + v \otimes w_2$. If V describes a quantum system and W another quantum system, then $V \otimes W$ describes both systems as a whole.

Examples:

1. The space V with $\dim V = 2$ and basis $B = \{v_1, v_2\}$. Then $V^{(2)} \equiv V \otimes V$ has the basis $\{v_1 \otimes v_1, v_1 \otimes v_2, v_2 \otimes v_1, v_2 \otimes v_2\}$. If the V space associated to some qubits has the basis $\{|0\rangle, |1\rangle\}$, then $V^{(2)}$ has the basis $|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

Complements of linear algebra

Operator functions

If A: $V \to V$ is a linear operator and f: $\mathbb{C} \to \mathbb{C}$ is a complex function (for example, a polynomial function), then the operator $f(A)$ is defined as: $f(A) : V \to V$.

Examples: For $f(z)z + 2$, $f(A) = A + 2I_V$ and for $f(z) = 3z^2 - 2z + 17$, $f(A) = 3A^2 - 2A + 17I_V$. Also in the case of a convergent power series $f(z) = c_0 + c_1 z + c_2 z + \cdots + c_n z^n + \cdots +$, $f(A) = c_0 I_V + c_1 A + \cdots + c_n A^n + \cdots$ (if the norm of the matrix is strictly less than the convergence radius of the series). For example, for $e^z = 1 + \frac{z}{1!} + \frac{z^2}{2!} + \cdots$, $e^A = I_V + \frac{A}{1!} + \frac{A^2}{2!} + \cdots$. If the matrices $A, B \in M_n(\mathbb{C})$ commute ($AB = BA$), then $e^A \cdot e^B = e^{A+B}$.

Assuming that $A : V \to V$ is a normal operator, having the spectral decomposition $A = \sum_i \lambda_i p_i$, where p_i is the projector $V \to V(\lambda_i)$ ($\sum_i p_i = I$, $p_i \circ p_j = \delta_{i,j} p_i$). Then the operator $f(A)$ is defined as:

$$f(A) = \sum_i f(\lambda_i) p_i. \tag{0.19}$$

Examples:

1. Let $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ be the Pauli matrix and $f(z) = e^z$. We consider the associated operator $A - \theta Z$, with real θ. The eigenvalues of A are $\lambda_1 - \theta$ and $\lambda_2 = -\theta$ and its eigenvectors are $v_1 - \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $v_2 - \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Then $\forall u - \begin{pmatrix} a \\ b \end{pmatrix}$, $p_1(u) = \langle v_1 | u \rangle v_1 = \begin{pmatrix} a \\ 0 \end{pmatrix}$ and $p_2(u) = \langle v_2\, u \rangle v_2 = \begin{pmatrix} 0 \\ b \end{pmatrix}$, so

$$e^{\theta Z} \begin{pmatrix} a \\ b \end{pmatrix} = e^{\theta} \begin{pmatrix} a \\ 0 \end{pmatrix} + e^{-\theta} \begin{pmatrix} 0 \\ b \end{pmatrix} = \begin{pmatrix} e^{\theta} a \\ e^{\ \theta} b \end{pmatrix} = \begin{pmatrix} e^{\theta} & 0 \\ 0 & e^{\ \theta} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \tag{0.20}$$

resulting in

$$e^{\theta Z} = \begin{pmatrix} e^{\theta} & 0 \\ 0 & e^{-\theta} \end{pmatrix} \tag{0.21}$$

2. Let $A = \begin{pmatrix} 4 & 3 \\ 3 & 4 \end{pmatrix}$ and $f(z) = \sqrt{z}$. Therefore $\lambda_1 = 7$, $\lambda_2 = 1$ and its eigenvectors $v_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, $v_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 \\ 1 \end{pmatrix}$. For $u = \begin{pmatrix} a \\ b \end{pmatrix}$, we have $p_1(u) =$

$\langle v_1|u\rangle v_1 = \frac{a-b}{2}\begin{pmatrix}1\\1\end{pmatrix}$ and $p_2(u) = \langle v_2|u\rangle v_2 = \frac{-a-b}{2}\begin{pmatrix}-1\\1\end{pmatrix}$, so $\sqrt{A}$ is the operator $\begin{pmatrix}a\\b\end{pmatrix} \mapsto \sqrt{1}\begin{pmatrix}\frac{a-b}{2}\\\frac{a-b}{2}\end{pmatrix} + 1\begin{pmatrix}\frac{a-b}{2}\\\frac{-a-b}{2}\end{pmatrix} = \frac{1}{2}\begin{pmatrix}\sqrt{1}-1 & \sqrt{1}+1\\\sqrt{1}+1 & \sqrt{1}-1\end{pmatrix}\begin{pmatrix}a\\b\end{pmatrix}$ so that $\sqrt{A} = \frac{1}{2}\begin{pmatrix}\sqrt{1}-1 & \sqrt{1}+1\\\sqrt{1}+1 & \sqrt{1}-1\end{pmatrix}$.

3. If $\vec{v} \in V_3$ is a versor and θ is a real number, then $e^{i\theta(\vec{v}\cdot\vec{\sigma})} = \cos(\theta)I + i\sin(\theta)(\vec{v}\cdot\vec{\sigma})$ where $\vec{\sigma}$ is a 3D vector.

Trace of an operator

If $A = (a_{ij})$; $1 \leq i, j \leq n$, then $\operatorname{Tr} A = \sum_i a_{ii}$.

Proposition 6. *(Trace properties).*

a). $\operatorname{Tr}(A + B) = \operatorname{Tr} A + TrB$ *and* $\operatorname{Tr}(cA) = c\operatorname{Tr}(A)$, $c \in \mathbb{C}$:

b). $\operatorname{Tr}(AB) = \operatorname{Tr}(BA)$;

c). If A is similar to B, then $\operatorname{Tr} A = \operatorname{Tr} B$ *(A and B have the same characteristic polynomial $P = (-1)^n x^n + c_1 x^{n-1} + \ldots$ and $\operatorname{Tr} A = \operatorname{Tr} B = c_1$). Therefore the trace is invariant to the similarity transformation $A \mapsto UAU^\dagger$.*

d). If $|v\rangle$ is a versor and $A : V \to V$ is a linear operator, then

$$\operatorname{Tr}(A|\psi\rangle\langle\psi|) = \langle\psi|A|\psi\rangle. \tag{0.22}$$

Examples:

1. The Pauli matrices X, Y, Z have 0 trace: $\operatorname{Tr}\sigma_i = 0$

2. Let L_V be the operator space of $V \to V$ (Hilbert space V). L_V is a complex linear space with a Hilbert space structure, defining $\langle A|A\rangle = \operatorname{Tr}(A^\dagger B)$ named Hilbert-Schmidt product. If $\dim(V) = n$, then $\dim(L_V) = n^2$.

The commutator of two operators

Definition 21. *Let $A, B : V \to V$ two linear operators. Their commutator is $[A, B] = AB - BA$ and their anti-commutator is $\{A, B\} = AB + BA$.*

Examples:

- $A\,B$ commute $\Leftrightarrow [A, B] = 0$
- $[X, Y] = 2iZ$, $[Y, Z] = 2iX$ and $[Z, X] = 2iY$. Renaming $X = \sigma_1$, $Y = \sigma_2$, $Z = \sigma_3 \Rightarrow \{\sigma_i, \sigma_j\} = 0 \forall i \neq j$ and $\sigma_i^2 = I$
- $[A, B]^\dagger = [B^\dagger, A^\dagger]$, $[A, B] = -[B, A]$.

- If A, B are hermitian matrices, then $i[A, B]$ is also hermitian.

Theorem (simultaneous diagonalization). *Let A and B be two hermitian operatos (self-adjoint operators). $[A, B] = 0 \Leftrightarrow$ there is an orthonormal basis $\mathcal{B}$ so that, $M_A^{\mathcal{B}}$, $M_N^{\mathcal{B}}$ are diagonal.*

Decomposition theorems

- **Polar decomposition** If $A \cdot V \to V$ is a linear operator, then U is a unitary operator and U and J are positive operators so that $K\ A - UJ - KU$, where J, K are unique operators ($J = \sqrt{A^\dagger A}$, $K = \sqrt{AA^\dagger}$). If A is also invertible, then U is also unique.
- **Spectral theorem** $A \in M_n(\mathbb{C})$ is normalized $\Leftrightarrow \exists$ a unitary U and a diagonal D so that $A = UDU^\dagger$.
- **Singular value decomposition**

  If $A \in M_n(\mathbb{C})$, then U and V are unitary matrices and D is a diagonal matrix for which $A = UDU^\dagger$.

Quantum Mechanics Crash Course

After introducing the minimal mathematical framework and the corresponding terminology, we will discuss more practically about the **quantum state space** and **observable** physical quantities (in the quantum context), as well as how observables are **measured.** Additionally, we will present the time evolution ($\equiv$ dynamics) of quantum systems and how they are assembled from small systems using tensor products. We will then delve into two of the fundamental, intimate mechanisms of quantum mechanics - superposition and entanglement, which challenge our senses.

Let us start with a short introduction to QM.[4]

Introduction

Until 1800, Mathematics and Physics were integrated into Natural Philosophy and were very closely connected. The great mathematicians (Newton, Lagrange, Fourier, Gauss) were well-informed about the physical hypotheses, theories, and experiments, and this continued into the period from 1850 to 1940 (with figures like Maxwell, Hertz, Poincaré, Hilbert, Dirac, Heisenberg, and von Neumann). In the meantime, crises unfolded in both mathematics (paradoxes that necessitated a rethinking of foundations and the development of Set Theory, Functional Analysis, and an analysis of the concept of computation) and physics (issues like the problem of the ether, resolved by Einstein, the "ultraviolet catastrophe," and the nature of

[4]This chapter follows the content of [5].

atomic spectra, among others). The study of light (treating it as both particles at the source and waves during propagation) explained diffraction and the photoelectric effect, solidifying the wave-particle duality model for all matter particles.

It is considered that the beginning of quantum mechanics was initiated by Max Planck in 1900 during a session of the German Physical Society. At that time, he demonstrated that energy, like matter, is composed of discrete units called "quanta." This idea was later reinforced by Albert Einstein in 1905 when he explained the photoelectric effect. According to Einstein's explanation, the interaction between light and matter occurs through discrete packets of energy called photons, which are actual particles that can be absorbed or emitted.

The goal of quantum physics is to study the elementary constituents of matter and processes whose characteristics (e.g., action) are related to Planck's constant. Physical quantities whose values can be experimentally measured, either directly or indirectly, such as energy, coordinates, momentum, spin, etc., are called **observables**. Microscopic entities cannot be directly measured, which is why various microscopic measurement devices are used. These devices are subject to inherent fluctuations, resulting in variable and random outcomes. Niels Bohr introduced the first model of the atom, viewing it as a planetary system with a nucleus surrounded by electrons that move in discrete orbits, jumping between these orbits and emitting or absorbing radiation. Until 1927, the physical foundations of quantum mechanics were established through the works of Heisenberg, de Broglie, and Dirac. The mathematical foundation was laid by von Neumann and Schrodinger through the theory of operators in Hilbert spaces and the theory of mathematical physics equations.

Quantum mechanics led to the development of atomic physics and later nuclear physics (after 1940), which included the construction of nuclear reactors and atomic bombs. It also played a crucial role in the study of elementary particles through the examination of high-energy particle collisions in particle accelerators. Additionally, various "civilian" applications emerged and developed, including the creation of polymers, semiconductors, superfluids, lasers, magnetic fluids, and more.

> Quantum mechanics has not only captivated the minds of physicists but also those of philosophers, biologists, and physiologists.

Bohr proposed the "Copenhagen interpretation" of quantum mechanics, which suggests that we cannot know the specific properties of particles, and until measured, they exist simultaneously in all possible states (the "principle of superposition"). Schrödinger introduced the "cat metaphor" in which a cat is placed in a thick lead box; when the box is sealed, we don't know if the cat is still alive, and the cat's state is simultaneously "dead and alive," in a superposition of states. When we open the box (this is the "measurement"!), the superposition collapses, and we find out whether the cat is dead or alive.

A recent interpretation of quantum mechanics is the "multiverse" theory, which suggests the existence of multiple possible worlds. As long as it's possible for a

physical object to exist in multiple states, it might exist in just as many "parallel universes," each containing a single state. Stephen Hawking and Richard Feynman have expressed support for such an interpretation. However, it's essential to note that this idea remains speculative and is a topic of debate and exploration in the field of theoretical physics.

The Standard Model

Quantum mechanics is distinct from quantum physics, just as it is distinct from quantum computers. Quantum physics explains nature using quantum mechanics, similar to how classical physics employs mathematics and experiments.

Currently, there are several axiomatization models of quantum mechanics: the Dirac-von Neumann axiomatization (called the "standard model"), statistical quantum mechanics, and quantum field theory. Here, we will refer to the standard model.

This includes 5 postulates (equivalent to axioms), also known as the principles of quantum mechanics.

> The principles of any field of knowledge are applied and discussed, but they are not questioned!

The 5 postulates form the theoretical basis of quantum systems (including quantum computers) and pertain to qubits, their measurements, and evolution, Schrödinger's law, and more. They were formulated by the early masters of the field, including Dirac, Heisenberg, von Neumann, around the 1930s. The postulates of quantum mechanics also demonstrate the connection between the physical world and the mathematical formalism of quantum mechanics.

> POSTULATE 1: "To every isolated quantum system Σ (e.g., electron, photon, atom, ion, particle family, etc.), there is associated a complex Hilbert space $H = H(\Sigma)$, called the **space of states of the system**, and non-zero states ψ of system Σ are represented by vectors $|\psi\rangle$ in H. If $\dim H = 2$, then the states are associated with qubits."

Comment: So, H is a complex linear space equipped with an inner product structure, with respect to which it is a complete metric space, with the distance $d(u, v) = \|u - v\|$. Any linear combination $\sum_k c_k|\psi_k\rangle$ of states with complex coefficients is called a **superposition** (= **overlapping**) of those states.

Finite-dimensional Hilbert spaces (isomorphic to spaces like $\mathbb{C}^n$ when equipped with a finite orthonormal basis) are used as spaces of localized degrees of freedom. This is the case with the 2D Hilbert space of electron spin states. The dimension of

the Hilbert space, denoted as H, typically corresponds to the number of basis states. In quantum mechanics, infinite-dimensional spaces with a countable orthonormal basis are also used, realized as spaces of square-integrable functions over spacetime.

Examples:

1. If $\dim_{\mathbb{C}} H = 2$ and $B = \{\mathbf{e}_0, \mathbf{e}_1\}$ is an orthonormal basis in H, then any state-vector $|\psi\rangle$ in H can be uniquely written as $|\psi\rangle = c_0\mathbf{e}_0 + c_1\mathbf{e}_1$ and can be identified with a qubit $\begin{pmatrix} c_0 \\ c_1 \end{pmatrix}$. Typically, we note $|\mathbf{e}_0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|\mathbf{e}_1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ are denoted as the **basis states**. Relative to the Euclidean inner product space, $\||\psi\rangle\|^2 = \langle\psi|\psi\rangle = \langle c_0|\mathbf{e}_0\rangle + c_1|\mathbf{e}_1\rangle | c_0|\mathbf{e}_0\rangle + c_1|\mathbf{e}_1\rangle\rangle = |c_0|^2 + |c_1|^2$. The quantum states associated with the quantum system are thus associated with qubits $|\psi\rangle = \begin{pmatrix} c_0 \\ c_1 \end{pmatrix}$ with $c_0, c_1 \in \mathbb{C}$ and $|c_0|^2 + |c_1|^2 = 1$. The real number $|c_0|^2$ (and $|c_1|^2$) is interpreted as the probability that $|\psi\rangle$ collapses into the basis state $|\mathbf{e}_0\rangle$ (and $|\mathbf{e}_1\rangle$), after the (somewhat mystical) measurement operation. These probabilities are also referred to as amplitudes. If $|\psi\rangle$ is a non-zero state and $c \in \mathbb{C}$, $c \neq 0$, then $|\psi\rangle$ and $c|\psi\rangle$ represent the same quantum state.

2. If $\dim_{\mathbb{C}} H = n$ $(n \geq 2)$ and $B = \{\mathbf{e}_0, \mathbf{e}_1, \ldots, \mathbf{e}_{n-1}\}$ is an orthonormal basis of H, then we obtain the basic quantum states

$$|\mathbf{e}_0\rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, |\mathbf{e}_1\rangle = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \ldots, |\mathbf{e}_{n-1}\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

and any state-vector $|\psi\rangle \in H$ is uniquely written

$$|\psi\rangle = \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix} \equiv \sum_k c_k|\mathbf{e}_k\rangle, \text{ with } \sum_k |c_k|^2 = 1.$$

The number $|c_k|^2$ is interpreted as the probability that $|\psi\rangle$ will collapse, after measurement, into the state $|\mathbf{e}_k\rangle$, $0 \leq k \leq n-1$.

Definition 22. *If $|\psi\rangle$ and $|\psi'\rangle$ are two normalized states ($\equiv$ unit vectors), then the inner product $A = \langle\psi|\psi'\rangle$ is called the transition amplitude from $|\psi\rangle$ to $|\psi'\rangle$. If $|\psi\rangle = (c_0, c_1, \ldots, c_{n-1})^{\mathsf{T}}$, $|\psi'\rangle = (c'_0, c'_1, \ldots, c'_{n-1})^{\mathsf{T}}$, then $A = \sum_k \overline{c_k}c'_k$. If the states are not normalized, then the corresponding amplitude is $A = \frac{\langle\psi|\psi'\rangle}{\||\psi\rangle\| \, \||\psi'\rangle\|}$. If the states $|\psi\rangle$ and $|\psi'\rangle$ are orthogonal, then $A = 0$, and it is said that the corresponding states **annihilate each other**.*

Examples: If $|\psi\rangle = \begin{pmatrix} 1 \\ 1-i \end{pmatrix}$, $|\upsilon'\rangle = \begin{pmatrix} i \\ -2 \end{pmatrix}$, then $\langle \upsilon' | \upsilon \rangle = (-i, -2) \begin{pmatrix} 1 \\ 1-i \end{pmatrix} = -2+i$ and $A = \frac{-2+i}{\sqrt{15}}$.

Let's consider a particle with mass m_1 located in three-dimensional space $\mathbb{R}^3$ equipped with spatial coordinates $\mathbf{x} = (x_1, x_2, x_3)$. We assume that the particle is moving under the influence of a potential $V = V(\mathbf{x})$. In this case, Quantum Mechanics recommends that the Hilbert space of states is the space $L^2(\mathbb{R}^3)$ of square-integrable functions $\psi(\mathbf{x})$, $\psi : \mathbb{R}^3 \to \mathbb{C}$ (meaning $\int_{\mathbb{R}^3} |\psi(\mathbf{x})|^2 d\mathbf{x} < \infty$, where $d\mathbf{x} = dx_1 dx_2 dx_3$), equipped with the inner product $\langle \phi | \upsilon \rangle = \int_{\mathbb{R}^3} \phi^*(\mathbf{x}) \upsilon(\mathbf{x}) d\mathbf{x}$. The energy of the particle is given by $E = \frac{p^2}{2m} + V(\mathbf{x})$, where p is the momentum.

Examples:

1. To define a classical bit, we consider a simple circuit: we associate the state $|1\rangle$ with a high voltage and the state $|0\rangle$ with a low voltage. Qubits, on the other hand, are simple quantum systems that can exist as superpositions of classical bits $|0\rangle$ and $|1\rangle$. For example, $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ is a superposition of classical bits $|0\rangle$ and $|1\rangle$ with amplitudes $\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}$.

2. Elementary particles have mass, electric charge, and also possess the property of spin (related to their rotation around their own axis). Electrons and positrons have spin $\frac{1}{2}$ (meaning they need to rotate twice to look the same), while photons have spin 1. In 1922, Germans Stern and Gerlach showed that in the presence of a magnetic field, an electron behaves like a "charged spinning top," acting as a tiny magnet that aligns itself with the external magnetic field (Figure 0.2).

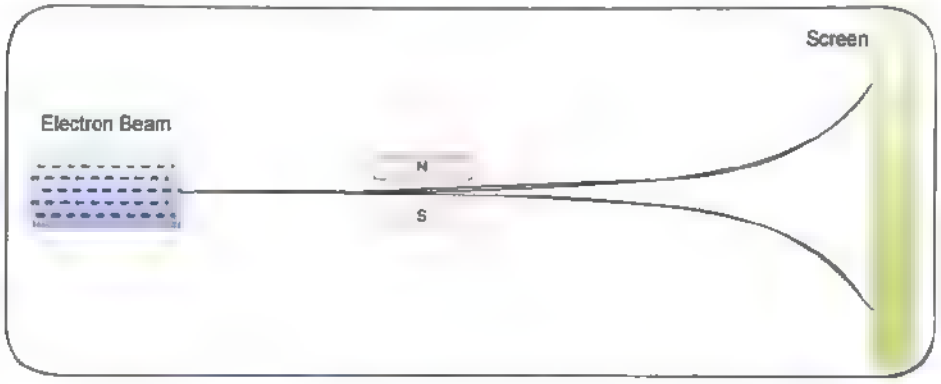


Fig. 0.2: Electrons act as "charged spinning tops", aligning with the magnetic field.

Sending a stream of electrons through a non-uniform magnetic field, oriented vertically, the field splits the flux into two fluxes with opposite spins, up $|\uparrow\rangle$ or down $|\downarrow\rangle$, hitting a screen. Surprisingly, all electrons end up only in these basic states (being rotated clockwise or counterclockwise), called spin-up and spin-down (in the case of fixing the vertical orientation of the magnetic field). The generic state of an electron will be of the form $|\upsilon\rangle = c_0|\uparrow\rangle + c_1|\downarrow\rangle$, with

$c_0, c_1 \in \mathbb{C}$ and $|c_0|^2 + |c_1|^2 = 1$, where $|c_0|^2$ (respectively $|c_1|^2$) is the probability that the electron collapses into the spin-up state (respectively spin-down). By convention, the state $|\uparrow\rangle$ is identified with $|0\rangle$ and $|\downarrow\rangle$ with $|1\rangle$, and thus the set $B = \{|\uparrow\rangle, |\downarrow\rangle\}$ is an orthonormal basis of the space $H \simeq \mathbb{C}^2$.

3. We consider a subatomic particle on an axis, and assume that the particle can only be detected at equidistant points $x_0, x_1, \ldots, x_{n-1}$, where $x_k = x_0 + ka$, $0 \leq k \leq n-1$. We associate these points with the basis states of the particle, expressed through ket vectors.

$$|x_0\rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, |x_1\rangle = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \ldots, |x_{n-1}\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix},$$

which form precisely the computational basis of the complex space $\mathbb{C}^n$. The particle can occupy any position along the axis, but we restrict ourselves to the **discrete**, finite-dimensional case. If $n \gg 1$ and a is an infinitesimal quantity, then we obtain the continuous case. Any state is of the form $|\psi\rangle = \sum_k c_k |x_k\rangle$, which is identified with the ket-vector $(c_0, c_1, \ldots, c_{n-1})^T$, representing a superposition of basis states. We have $\|\psi\|^2 = \sum_k |c_k|^2$, and the numbers $p(x_k) = \frac{|c_k|^2}{\|\psi\|^2}$ are interpreted as the probabilities that, upon observation (measurement) of the particle, it will be detected at position x_k $(0 \leq k \leq n-1)$, meaning in one of the basis states.

Example: Let $n = 4$ and $|\psi\rangle = (1-i, 2i, 5, 0)^T$. The probability for the particle to be observed in the position x_2 is $\frac{25}{31} \approx 0.9$, because $\|\psi\|^2 = 31$.

Question: Who chooses the space $H = H(\Sigma)$?

Answer: It is up to the physicist to specify (to choose) the Hilbert space of states, either by following existing models or by imagining new ones.

> POSTULATE 2: "If the quantum system Σ does not interact with other systems and is in a non-zero state $|\psi_0\rangle$ at a moment t_0, then it transitions to another non-zero state $|\psi_1\rangle$ at time t_1 with a probability equal to the real subunitary number $\cos^2 \alpha$, where α is the measure of the angle $\widehat{\psi_0, \psi_1}$ between the states $|\psi_0\rangle$ and $|\psi_1\rangle$; moreover, these two states are connected by a unitary operator $U : H \to H$ $(U^\dagger U = I)$, which depends **only** on the moments t_0, t_1, namely: $|\psi_1\rangle = U(|\psi_0\rangle)$."

Comment: This postulate reveals two things: how the states of the system Σ change over time and the fact that this evolution is described by unitary operators. In the Hilbert space $H = H(\Sigma)$, we have $\cos\alpha = \frac{\langle \psi_0 | \psi_1 \rangle}{\|\psi_0\| \cdot \|\psi_1\|}$, where α lies in the interval

$[0, \pi]$, so $\cos\alpha$ is equal to the absolute value of the transition amplitude of the system Σ from $|\upsilon_0\rangle$ to $|\upsilon_1\rangle$. If $\alpha = \frac{\pi}{2}$, then the system cannot transition from $|\upsilon_0\rangle$ to $|\upsilon_1\rangle$ or vice versa.

Examples:

1) If $|\upsilon\rangle = a|0\rangle + b|1\rangle$ and $U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, then $U|\upsilon\rangle = U \cdot \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} b \\ a \end{pmatrix} = b|0\rangle + a|1\rangle$. It is said that this U "flips." In contrast, the operator $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, for which $Z|0\rangle = |0\rangle$ and $Z|1\rangle = -|1\rangle$ "flips the phase".

2) Let $|\upsilon\rangle = 1|0\rangle + 0\,1\rangle = 1 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + 0 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and the Hadamard matrix $U = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, which is unitary. Then $U|\upsilon\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. The transition probability from $|\upsilon\rangle$ to $|\upsilon_1\rangle = U|\upsilon\rangle$ is $\cos^2\alpha$. But $|\upsilon\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|\upsilon_1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ so $\langle\upsilon|\upsilon_1\rangle = \frac{1}{\sqrt{2}}$, $\|\upsilon\| = 1$, $\|\upsilon_1\| = 1$ and such as, $\cos\alpha = \frac{1}{\sqrt{2}}$, but the transition probability is $\frac{1}{2}$.

POSTULATE 3: "Any measurable quantity, with measurable values on the states of the isolated system Σ, is bijectively associated with a self-adjoint operator, and if $\dim H < \infty$, with a Hermitian matrix A ($A = A^\dagger$), whose eigenvalues (real, according to Proposition 3 in Chapter 1) are the only values obtained by measuring on various states of the corresponding observable. Furthermore, if $|\upsilon\rangle \in H$ is an eigenvector for A, with eigenvalue λ, then by measuring the observable, the value λ is precisely obtained with probability 1. Quantum measurements are described by a collection $\{M_m\}$ of measurement operators $M_m : H \to H$ (non unitary!), which act on the system's states (the index "m" refers to measurement events). If the state of the Σ system is $|\upsilon\rangle$ before the measurement, then the probability of obtaining "m" is

$$p(m) = \langle\upsilon|M_m^\dagger M_m|\upsilon\rangle \qquad \left(1 = \sum_m p(m)\right). \tag{0.23}$$

and the state after measurement will be

$$\frac{M_m|\psi\rangle}{\sqrt{p(m)}}. \tag{0.24}$$

Therefore, $\sqrt{p(m)} = \|M_m|\psi\rangle\|$ and $\sum_m M_m^\dagger M_m = I$ ("completeness relation"):

Comments and additions: The entire field of science is based on observations of various quantities and the development of scientific concepts. Physics, in particular, has accumulated many quantifiable observations that have been elevated to the status of confirmed theoretical results and principles concerning various fundamental quantities such as mass, velocity, momentum, energy, spin, etc. Quantum systems are studied through the space of states and the set of observables (i.e., physical quantities that can be observed/measured in various states), addressing questions like what values can be observed/measured and how these quantities evolve over time. Any observable $f : H \to H$ is an operator that transforms one state $|\psi\rangle$ into another state $f|\psi\rangle$.

By measuring a quantum system in a certain state, classical (not quantum) information about that state is obtained. The act of measuring a physical system in an unknown state irreversibly destroys that state, which cannot be recovered. A quantum system can only be observed/measured in its basic states, and it can exist in any superposition of these basic states as long as it is not measured.

> Measurement is the only non-unitary operator that a quantum computer can execute during a quantum computation.

Examples:

1) Let $H \simeq \mathbb{C}^2$ the state space of a spin and a spin in the state $|\psi\rangle = 2|\uparrow\rangle + 3i|\downarrow\rangle$. We demonstrate that the operator $f : \mathbb{C}^2 \to \mathbb{C}^2$, $(x, y) \mapsto (x + iy, -ix + y)$ is self-adjoint and determine its transformation on $|\psi\rangle$ through f.

   The matrix of f in the computational (canonical) basis of $\mathbb{C}^2$, it is $F = \begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix}$, and it is evidently Hermitian, with eigenvalues $\lambda_1 = 0$ and $\lambda_2 = 2$.

   Then, $f|\psi\rangle = F|\psi\rangle = \begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 3i \end{pmatrix} = \begin{pmatrix} -1 \\ i \end{pmatrix} = -1|\uparrow\rangle - i|\downarrow\rangle$.

2) We consider the following two operators of the space $\mathbb{C}^2$: $M_0 = |0\rangle\langle 0|$, $M_1 = |1\rangle\langle 1|$. We prove the completeness relation: $M_0^\dagger M_0 + M_1^\dagger M_1 = I$ and determine the states of the 1-qubit $|\psi\rangle = a|0\rangle + b|1\rangle$ after measurements $m = 0$ and $m = 1$".

   We have $M_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}(1 \;\; 0) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $M_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}(0 \;\; 1) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ so $M_0^\dagger M_0 + M_1^\dagger M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$. It is observed that the operators M_0, M_1 are self-adjoint, and we have $M_0^2 = M_0$ and $M_1^2 = M_1$. Thus, we have two measurement operators with indices $m = 0$, $m = 1$.

We measure the state $|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$ for $m = 0$. According the relation (0.23),

$$p(0) = \left\langle \psi \left| M_0^\dagger M_0 \right| \psi \right\rangle = \langle \psi | M_0 | \psi \rangle = (\bar{a}, \bar{b}) \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a \\ b \end{pmatrix} = (\bar{a} \quad 0) \begin{pmatrix} a \\ b \end{pmatrix} = |a|^2$$

so the probability of measuring $|0\rangle$ is the amplitude $|a|^2$: similarly $p(1) = (\bar{a}, \bar{b}) \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = |b|^2$. The state to which $|\psi\rangle$ passes after measurement $m = 0$ is, according to (0.24), $\frac{M_0 \psi}{\|M_0 \psi\|} = \frac{a}{|a|}|0\rangle$ and similarly, the state after measurement $m = 1$ is $\frac{M_1|\psi\rangle}{\|M_1|\psi\rangle\|} = \frac{b}{|b|}|1\rangle$.

3) Let a (non-relativistic) particle located on an axis, the state space being $H = \left\{ \psi : \mathbb{R} \to \mathbb{C} \mid \psi \text{ derivable and } \int_{\mathbb{R}} \psi(x)^2 < \infty \right\}$, $\dim_{\mathbb{C}} H = \infty$, with scalar product: $\langle \phi, \psi \rangle = \int_{\mathbb{R}} \overline{\phi(x)} \psi(x)\, dx$. There are two remarkable observables $P : H \to H$, $\psi(x) \mapsto \psi'(x)$ and $Q : H \to H$, $\psi(x) \mapsto x\psi(x)$. We calculate the commutator of $[P, Q] = P \cdot Q - Q \cdot P$.

We have $[P, Q](\psi) = P(Q(\psi)) - Q(P(\psi)) = P(x\psi(x)) - Q(\psi'(x)) = \psi(x) + x\psi'(x) - x\psi'(x) = \psi(x)$ so $[P, Q] = 1_H$.

> In quantum mechanics, the fact that two operators associated with observables do not commute implies that the corresponding observables cannot be measured simultaneously.

Returning to example 3, because $[P, Q] \neq 0$, it follows that the observables P and Q cannot be measured simultaneously.

4) In the case of a non-relativistic particle in three-dimensional space $\mathbb{R}^3$ with respect to an orthonormal reference frame $Ox_1x_2x_3$, subject to the influence of a potential $V(x_1, x_2, x_3)$, the Hilbert space of the particle's states is given by

$$H = \left\{ \psi : \mathbb{R}^3 \to \mathbb{C} \mid \psi \in C^1(\mathbb{R}^3), \int_{\mathbb{R}^3} |\psi(x_1, x_2, x_3)|^2 dx_1 dx_2 dx_3 < \infty \right\},$$

with scalar product $\langle \phi, \psi \rangle = \int_{\mathbb{R}^3} \overline{\phi(x_1, x_2, x_3)} \psi(x_1, x_2, x_3)\, dx_1 dx_2 dx_3$.

In this case, three observables of position can be defined, associated with the operators $Q_j : \psi(\mathbf{x}) \mapsto x_j \cdot \psi(\mathbf{x})$, $1 \leq j \leq 3$ and another three observables of momentum, through the operators

$$P_j : \psi(\mathbf{x}) \mapsto \frac{\hbar}{i} \cdot \frac{\partial}{\partial x_j} \psi(\mathbf{x}), \, 1 \leq j \leq 3,$$

where $\hbar \approx 1.055 \times 10^{-34}$ [Js] is the reduced Planck constant, which has the dimensions of action (energy × time). Using the commutator of two operators, $[A, B] = A \cdot B - B \cdot A$, the following "commutation relations" can be demonstrated:

$$[P_j, P_k] = 0,\ [Q_j, Q_k] = 0,\ [P_j, Q_k] = \frac{\hbar}{i}\delta_{jk},\ 1 \leq i, j, k \leq 3$$

5) Fixing an orthonormal coordinate system $Oxyz$, Pauli defined three famous spin operators:

$$S_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ S_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},\ S_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

sometimes denoted as X, Y, Z, which describe the mode of rotation of particles. For example, in the case of S_z, the orthonormal basis is $\{|\uparrow\rangle, |\downarrow\rangle\}$, so rotation in the Oz direction is "up" or "down"; in the case of S_x, the orthonormal basis is $\{|\leftarrow\rangle, |\rightarrow\rangle\}$, and rotation is in the Ox direction "to the left" or "to the right". Through direct calculation, we obtain the following relationships:

$$[S_x, S_y] = 2iS_z,\ [S_y, S_z] = 2iS_x,\ [S_z, S_z] = 2iS_y.$$

In general, if $A_1, A_2 \in M_n(\mathbb{C})$ are Hermitian, then the product $A_1 \cdot A_2$ is Hermitian if and only if they commute, meaning $[A_1, A_2] = 0$. In particular, if A is Hermitian, then its powers A^k, $k \geq 2$, are also Hermitian.

Since $[S_x, S_y] \neq 0$, results in the product S_xS_y is not a Hermitian matrix.

Additional clarifications

If $A \in M_n(\mathbb{C})$ is a Hermitian matrix associated with an observable, then $\forall u \in \mathbb{C}^n$, the scalar product $\langle Au \quad u\rangle$ is a real number (because $\langle Au \mid u\rangle = \langle u \mid Au\rangle = \langle Au \mid u\rangle^*$).

Definition 23. *If $|v\rangle \in H(\Sigma)$ and A is an observable, then the real number*

$$A_v = \langle A|\psi\rangle \mid |\psi\rangle\rangle = \psi^\dagger \cdot A \cdot \psi$$

is called ***the average of the observable A on the state*** *$|v\rangle$ (simply denoted as ψ).*

Proposition 7. *Let λ_k the eigenvalues of A, $H = \underset{k}{\oplus} V(\lambda_k)$ and projectors $p_k : H \to V(\lambda_k)$. If $|\psi\rangle \in H$, then*

$$A_\psi = \sum_k \lambda_k \|\psi_k\|^2,\ |\psi_k\rangle = p_k(\psi). \tag{0.25}$$

Demonstration. We have $|\upsilon\rangle = \sum_k |\upsilon_k\rangle$ and $|\upsilon|^2 = \sum_k \|\upsilon_k\|^2$. According to the Spectral Theorem (relation (0.12) from Chapter 1). $A = \sum_k \lambda_k p_k$ for the operator of observable A and $\langle \upsilon \mid \upsilon_j \rangle = \langle \sum_k \upsilon_k | \upsilon_j \rangle = \|\upsilon_j\|^2$ so $A_\upsilon = \langle A\upsilon \mid \upsilon \rangle = \langle \upsilon \mid A\upsilon \rangle = \langle \psi | \sum_k \lambda_k p_k | \psi \rangle \rangle = \sum_k \lambda_k \langle \psi | \psi_k \rangle = \sum_k \lambda_k \|\psi_k\|^2$. □

Interpretation: By considering a random variable with the probability distribution matrix $\begin{pmatrix} \lambda_k \\ \|\psi_k\|^2 \end{pmatrix}$, it follows that A_υ is the mean of this random variable Denoting $m = A_\upsilon$. it makes sense to define the observable $B = (A - mI)^2$; in general, if A is a self-adjoint operator. then the operators A^k, $A - \alpha I$, $(A - \alpha I)^k$, $k \geq 2$ are also self-adjoint.

Definition 24. *The mean of B_υ is called the* ***dispersion*** *(≡* ***variance****) of the observable values of A in the state υ. denoted as $D_\upsilon A$.*

A famous result is given by the following the

Theorem (Heisenberg Uncertainty Principle). *"For any two observables A, B : $H \to H$ $(H = H(\Sigma))$ and for any state vector $\psi \in H$,*

$$(D_\psi A) \cdot (D_\psi B) \geq \frac{1}{2} |\langle C(\psi) | \psi \rangle|, \tag{0.26}$$

where $C = [A, B] = A \cdot B - B \cdot A$."

The demonstration is more technical. and we prefer to provide more examples.

Note: From inequality (0.26). it follows that both dispersions cannot be minimized simultaneously. The commutator C indicates a limit on measurement precision and shows how good a simultaneous measurement of two observables can be. If $C = 0$ (zero). meaning A and B commute. then the product of dispersions can become arbitrarily large. Applying Heisenberg's uncertainty theorem , for $A = S_x$ and $B = S_y$ (which do not commute!). we can estimate the accuracy of simultaneously measuring the spin in the Oz and Ox directions.

Examples:

1) Let $A = \begin{pmatrix} 1 & -i \\ i & 2 \end{pmatrix}$ and $|\upsilon\rangle = \begin{pmatrix} i/\sqrt{2} \\ -i/\sqrt{2} \end{pmatrix}$ so $A|\upsilon\rangle = \begin{pmatrix} 1 & -i \\ i & 2 \end{pmatrix} \begin{pmatrix} i/\sqrt{2} \\ -i/\sqrt{2} \end{pmatrix} - \begin{pmatrix} \frac{-1+i}{\sqrt{2}} \\ \frac{-1-2i}{\sqrt{2}} \end{pmatrix}$ and results in $A_\upsilon = \langle A_\upsilon \mid \upsilon \rangle = \frac{-1-i}{\sqrt{2}} \frac{i}{\sqrt{2}} + \frac{-1-2i}{\sqrt{2}} \left(-\frac{i}{\sqrt{2}} \right) = -\frac{1}{2}$.

2) Let $A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ with $a, b \in \mathbb{R}$ and $|\upsilon\rangle = \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}$. We denote by $m = A_\psi$ (so $(A - mI)^2 = \begin{pmatrix} (a-m)^2 & 0 \\ 0 & (b-m)^2 \end{pmatrix}$ and $D_\upsilon A = \begin{pmatrix} \overline{c_1} & \overline{c_2} \end{pmatrix} \begin{pmatrix} (a-m)^2 & 0 \\ 0 & (b-m)^2 \end{pmatrix}$

$\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = (a - m)|c_1|^2 - (b-m)^2 c_2|^2$. If values a, b are "close" to m then $D\psi A \approx 0$. In particular, for $S_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, we have $a = 1, b = -1$ and for $|\psi\rangle = \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}$ and the expectation value of the observable S_z on the state vector is $m = (\overline{c_1}, \overline{c_2}) \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = c_1|^2 - |c_2|^2$ and we obtain $D_\psi S_z = (\overline{c_1} - \overline{c_2}) \begin{pmatrix} (1-m)^2 & 0 \\ 0 & (1+m)^2 \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = |c_1|^2 (1-m)^2 + |c_2|^2 (1+m)^2 = 1 + m^2 + 2m\left(|c_2|^2 - |c_1|^2\right) = 1 + m^2 - 2m^2 = 1 - m^2$. This is maximum if $m = 0$, so $|c_1| = |c_2|$. Because $|c_1|^2 + |c_2|^2 = 1$, one of the solutions is $|\psi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\rangle$.

Postulate 3 also applies to quantum measurements. In physics, specific states are characterized by determining the values of observable quantities (such as energy, spin, field, coordinates, etc.): it is then said that those quantities are **measured**. By choosing measurement units and origins ("zeros"), the respective values are certain real numbers or scalar quantities.

Example: In classical physics, observation/measurement leaves the system in the state it was in, and the result is predictable. However, in the quantum world, the systems themselves are perturbed by measurements, and measurements are random processes. According to Postulate 3, we know that an observable can only take one of its eigenvalues as a result of measurement, but we do not know how frequently a specific eigenvalue occurs. Let

$$A = \begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix}, \; |\psi\rangle = \begin{pmatrix} -1 \\ -1 - i \end{pmatrix}.$$

Then $|\psi_1\rangle = A|\psi\rangle = \begin{pmatrix} i \\ -1 - 2i \end{pmatrix}$ and $|\psi_1\rangle \neq |\psi\rangle$ so the state has changed. The eigenvalues of A are $\pm\sqrt{2}$: for $\lambda_1 = \sqrt{2}$ and $\lambda_2 = -\sqrt{2}$, the corresponding eigenvectors are

$$|e_1\rangle \approx \begin{pmatrix} -0,92i \\ -0,38 \end{pmatrix}, \; |e_2\rangle \approx \begin{pmatrix} -0,38 \\ 0,92i \end{pmatrix}.$$

If the observation of A is performed on another state, and the observed value is λ_1, then according to Postulate 3, the system "collapses" to either $|e_1\rangle$ or $|e_2\rangle$.

So if we measure an observable, the system transitions to the corresponding eigenvector, and if immediately after that measurement, we make another one, the system will remain where it is. If we measure multiple observables, the order of measurements matters.

Note: In the case when $\dim H < \infty$, the eigenvalues of a self-adjoint operator $A : H \to H$ are finite in number and form a discrete spectrum. But if $\dim H = \infty$,

the spectrum can be continuous, and in this case, the operator A **has a spectral resolution**, which means it has an increasing system of projectors (P_a), $a \in \mathbb{R}$ that commute with each other and satisfy $\lim_{a \to -\infty} P_a = 0$, $\lim_{a \to +\infty} P_a = I_H$ and $A = \int_{\mathbb{R}} a dP_a$ (in the Stieltjes sense). However, we stop here because we are entering the field of functional analysis.

> Many statements in quantum mechanics are of a probabilistic nature because in the quantum world, strict causality doesn't exist. Quantum particles don't have well-defined trajectories, and furthermore, in a system with two identical particles, they cannot be distinguished (for example, we can't label them as particle 1 and particle 2). Such discussions began in the 1920s and have not yet concluded!

The first three postulates of quantum mechanics have referred to states, observables, and measurements, related to **static** quantum systems that do not evolve in time. However, quantum systems cannot be considered independent of time; they are not stationary. Changes and alterations of state are the result of various measurements, so quantum systems are inherently **subject to dynamics.**

> As self-adjoint operators (= Hermitian operators) are associated with physical observables, similarly, unitary operators determine the dynamics of systems.

Before formulating the other two principles of quantum mechanics, some preparations are necessary...

We recall that $\forall z \in \mathbb{C}$, the complex exponential is defined as $e^z \equiv \exp(z) = 1 + \frac{z}{1!} + \frac{z^2}{2!} + \cdots + \frac{z^n}{n!} + \ldots$, where the series is convergent; clearly, $\exp(0) = 1$, $\exp(z)\exp(z') = \exp(z + z')$ and $\exp(z)^{-1} = \exp(-z)$. Certainly, this yields the famous Euler's formula: $e^{ix} = \cos x + i \sin x$, for all $x \in \mathbb{R}$. The function $\exp : \mathbb{C} \to \mathbb{C}$ is periodic with a period of $2\pi i$.

Then, for any linear operator $f : H \to H$ (where h is a complex Hilbert space), it can be defined the **exponential of** f as the operator $e^f \equiv \exp(f) = I_H + f + \frac{f^2}{2!} + \cdots + \frac{f^n}{n!} + \ldots$, where $f^n = f \circ f \circ \cdots \circ f$ (composed n times). We have $e^0 = I_H$, and if the linear operators $f, g : H \to H$ commute, then $\exp(f)\exp(g) = \exp(f + g)$ and $\exp(f)$ is invertible with $\exp(f)^{-1} = \exp(-f)$. In addition,

$$\frac{d}{dt}\left(e^{tf}\right) = \left(I_H + tf + \frac{t^2 f^2}{2!} + \cdots + \frac{t^n f^n}{n!} + \ldots\right)' = f + tf^2 + \cdots + \frac{t^{n-1}}{(n-1)!} f^n + \ldots$$

adică

$$\frac{d}{dt}\left(e^{tf}\right) = f \circ e^{tf} = e^{tf} \circ f. \tag{0.27}$$

POSTULATE 4: "The self-adjoint operator $\mathcal{H}$ representing the observable energy is the Hamiltonian of the quantum system Σ. $\mathcal{H} : H(\Sigma) \to H(\Sigma)$, determined by the physicist. The eigenvalues (real!) of $\mathcal{H}$ constitute the energy spectrum of Σ. If at time t, the system is in the state $|\psi\rangle$, and no measurements are made on the Σ system (assumed isolated), then at any other time t, the system will be in the state

$$|\psi(t)\rangle = U(t)|\psi\rangle, \text{ where } U(t) = \exp\left(\frac{i}{\hbar}t\mathcal{H}\right)." \tag{0.28}$$

The operator $U(t) : H \to H$ given by (0.28) satisfies the relations: $U(0) = I_H$ and $\forall t \in \mathbb{R}$, $U(t) \circ U(-t) = I_H$. In addition, $U(t)$ is unitary (i.e., $U(t) \circ U(t)^{\dagger} = I_H$) and $U(t)^{\dagger} = U(-t)$.

Proposition 8 (The properties of the Hamiltonians). *1. The set $\{U(t) \mid t \in \mathbb{R}\}$ is a group under composition, called the one-parameter group of unitary operators on the space H, generated by the Hamiltonian $\mathcal{H}$.*

2. This group completely determines the evolution of the system Σ.

3. For any $t \in \mathbb{R}$, the Schrödinger equation holds:

$$|\psi'(t)\rangle = -\frac{i}{\hbar}\mathcal{H}(|\psi(t)\rangle). \tag{0.29}$$

Demonstration. 1. It easily verifies the group axioms.

2. Indeed, starting from a state $\psi(t)$ of Σ at a certain time t, we can determine the state of Σ at any other moment: $\psi(\tau) = U(\tau - t)|\psi(t)\rangle$.

3. We differentiate equation (0.28) with respect to t:

$$|\psi'(t)\rangle = \exp\left(-\frac{i}{\hbar}t\mathcal{H}|\psi(t)\rangle\right) \circ \left(-\frac{i}{\hbar}\mathcal{H}\right).$$

□

Note: Equation (0.29) of Schrödinger gives the time evolution law of quantum states for the quantum system Σ. Multiplying by i, equation (0.29) can be equivalently written as: $i\hbar|\psi'(t)\rangle = \mathcal{H}|\psi(t)\rangle$.

Example (1D Harmonic Oscillator): In classical mechanics, we consider a point particle moving along an axis, attracted towards the origin by a force proportional to the distance x between the particle and the origin. The kinetic energy is $\frac{mv^2}{2} = \frac{p^2}{2m}$ (since $p = mv$), and the total energy is $E = \frac{p^2}{2m} + V(x)$, which is constant.

The time evolution of the classical oscillator is well-known from classical rational mechanics.

In the quantum version, the associated Hilbert space is $L^2(\mathbb{R})$, which consists of square-integrable functions $\psi(x)$, where $\psi : \mathbb{R} \to \mathbb{C}$, and $\int_{\mathbb{R}} |\psi(x)|^2 dx < \infty$. This space is equipped with the inner product: $\langle \phi | \psi \rangle = \int_{\mathbb{R}} \overline{\phi(x)} \psi(x) dx$. By introducing the momentum operator P and the position operator Q, we obtain the energy operator (Hamiltonian)

$$\mathcal{H} = \frac{P^2}{2m} + \frac{1}{2} m\omega^2 Q.$$

The eigenvalues of this operator are $E_n = n\hbar\omega$, which correspond to the discrete energy levels. The oscillator has a lowest non-zero energy, namely $E_1 = \hbar\omega$, which is called the "zero point energy".

Note: There is a discrete (≡ "stepped") version of Postulate 4, which is used in quantum calculations, namely:

POSTULATE 4′: "The evolution of a discrete quantum system Σ is determined by a unitary operator U, such that if the system's state at time t is $|\psi(t)\rangle$, then the state at time $t+1$ is

$$|\psi(t+1)\rangle = U|\psi(t)\rangle. \tag{0.30}$$

In addition, the discrete version of the Schrödinger equation states that the rate of change of the state $|\psi(t)\rangle$ is equal to $-\frac{i}{\hbar}\mathcal{H}|\psi(t)\rangle$; solving this equation, with certain initial conditions, determines the time evolution of the Σ system."

We assume that we have a sequence of moments $t_0, t_1, \ldots, t_{n-1}$ and that at each moment t_k, a unitary matrix $U(t_k)$ is fixed. Starting from an initial state $|\psi_0\rangle$, the states $|\psi_1\rangle = U(t_0)|\psi_0\rangle$, $|\psi_2\rangle = U(t_1)|\psi_1\rangle$, and so on, are successively determined; this sequence is called the **orbit** of $|\psi_0\rangle$. The evolution is symmetric with respect to time, applying the adjoint / inverses $U(t_k)^\dagger$ of the matrices $U(t_k)$.

We will see in Chapters 3 and 4 că that a quantum computer is placed in an initial state, and then a sequence/chain of unitary operators (through quantum gates) is applied to this state. By measuring the output of this chain, the final state is obtained.

POSTULATE 5: "If Σ_1, Σ_2 are two independent and isolated quantum systems, then the state space of the **composite** ($\equiv$ **assembled, merged**) quantum system Σ is the tensor product of the state spaces of the component systems, meaning:

$$H(\Sigma) = H(\Sigma_1) \otimes H(\Sigma_2). \tag{0.31}$$

In addition, if Σ_1 is in the state $|\psi_1\rangle$ while Σ_2 is in state $|\psi_2\rangle$, then Σ will be in the state $|\psi_1\rangle \otimes |\psi_2\rangle$. Relation (0.31) extends to any composite quantum systems $\Sigma_1, \ldots, \Sigma_n$ whose composite system is Σ; specifically,

$$H(\Sigma) = H(\Sigma_1) \otimes H(\Sigma_2) \otimes \cdots \otimes H(\Sigma_n)." \tag{0.32}$$

Examples:

1) If Σ_1 is in the state $|\psi_1\rangle = a|0\rangle + b|1\rangle$ and Σ_2 is in the state $|\psi_2\rangle = c|0\rangle + d|1\rangle$, then the composite system will be in the state $|\psi_1\rangle \otimes |\psi_2\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix} = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle$.

2) Assuming that one particle is located along an axis with positions $\{x_0, x_1\}$, forming the system Σ_1, and another particle is located, possibly along a different axis, with positions $\{y_0, y_1\}$, forming the system Σ_2. By assembling (combining) the systems Σ_1 and Σ_2, we obtain 4 basis states $|x_0\rangle \otimes |y_0\rangle$, $|x_0\rangle \otimes |y_1\rangle$, $|x_1\rangle \otimes |y_0\rangle$ and $|x_1\rangle \otimes |y_1\rangle$, which generate the tensor product $H(\Sigma_1) \otimes H(\Sigma_2)$. Any state $|\psi\rangle$ of the composite system is a superposition of these basis states, which can be assimilated to a vector in $\mathbb{C}^4$: $|\psi\rangle = c_{00}|x_0 \otimes y_0\rangle + c_{01}|x_0 \otimes y_1\rangle + c_{10}|x_1 \otimes y_0\rangle + c_{11}|x_1 \otimes y_1\rangle$. The quantity $|c_{ij}|^2$ represents the probability of finding the particles at the positions x_i, y_j. For example, if $|\psi\rangle = 3i|x_0\rangle \otimes |y_0\rangle - 2|x_1\rangle \otimes |y_0\rangle + (1-i)\,x_1\rangle \otimes |y_1\rangle$, then the probability that the first particle is at position x_1 and the second particle is at position y_0 is given by

$$p_{10} = \frac{|-2|^2}{|3i|^2 + |-2|^2 + |1+i|^2} = \frac{4}{15}.$$

Question: Why are tensor products used?

Answer: The operation "$\otimes$" describes the essence of composition, also related to entanglement: if a system Σ_1 is in the state $|o\rangle$ and system Σ_2 in the state $|\psi\rangle$,

then $\phi\rangle \otimes |v\rangle$ contains something from Σ_1 and something from Σ_2. If we have one measurement with n outputs and another with m outputs, then the product system has $n \times m$ outputs, so the associated Hilbert space has the product dimension, not the sum. Thus, the Kronecker or tensor product is used. Separable states form the sum space, and the difference (with $n \times m - m - n$ dimensions) is given by entangled states

The previous example extends to composing systems with n basis states, $x_0, x_1, \ldots, x_{n-1}$, with other systems having m basis states, $y_0, y_1, \ldots, y_{m-1}$.

Note: Postulate 5 is also called the "quantum assemblage postulate". We have previously discussed the "quantum inseparability" ("entanglement") of quantum states. This fundamental operation in quantum mechanics, as well as in quantum computing, encourages us to depart from the idea that composite systems can only be understood through their constituents. The basis states of a system $\Sigma_1 \otimes \Sigma_2$ are the tensor products of the basis states of these component systems. It would have been convenient if any state of $\Sigma_1 \otimes \Sigma_2$ (not just the basis states) could be the tensor product of a state of Σ_1 and one of Σ_2, but this is not the case!

Example: Let $|v\rangle = |x_0\rangle \otimes |y_0\rangle + |x_1\rangle \otimes |y_1\rangle$. If $|v\rangle$ were the tensor product of two states $|\psi_1\rangle = a|x_0\rangle + b|x_1\rangle$, $|v_2\rangle = c|y_0\rangle + d_1|y_1\rangle$ of the systems Σ_1, Σ_2, then it would follow that $ac = 1$, $ad = 0$, $bc = 0$, $bd = 1$, which are contradictory relationships (because $c \neq 0$ implies $b = 0$); therefore, the state $|v\rangle$ is entangled. Going further, if we measure the first particle, the probability for it to be in position x_0 is $\frac{1}{\sqrt{2}}$, and similarly for position x_1. Then $p(x_0, y_1) = 0$, so if the first particle is in position x_0, the second one cannot be in position y_1. Thus, the individual states of the two particles are intimately connected, and measuring one will determine the measurement of the other!

But if we had started with the state $|v\rangle = |x_0\rangle \otimes |y_0\rangle - |x_0\rangle \otimes |y_1\rangle + |x_1\rangle \otimes |y_0\rangle + |x_1\rangle \otimes |y_1\rangle$ or with $|\psi\rangle = |x_1\rangle \otimes |y_0\rangle + |x_1\rangle \otimes |y_1\rangle$, the previous example would not have worked.

Question: Why?

Answer: In the first case, $|v\rangle = |v_1\rangle \otimes |v_2\rangle$, where $|v_1\rangle = |x_0\rangle + |x_1\rangle$ and $|v_2\rangle = |y_0\rangle + |y_1\rangle$, and in the second case, $|v\rangle = |x_1\rangle \otimes (|y_0\rangle + |y_1\rangle)$.

We will see that entanglement plays a special role in the design of quantum algorithms and in teleportation (the transfer of quantum states from one location to another).

For the study of systems with a large number of particles (for example, a container of gas), it is impossible and unproductive to study the motion of individual particles separately. In such cases, the properties of interest are global properties (such as temperature or pressure), shifting the focus from states to observables.

Review: Postulate 1 refers to the Hilbert space associated with any isolated quantum system (including qubits in particular); Postulate 2 concerns the transformation of qubits, and Postulate 3 deals with the effect of measurements. The last two postulates summarize the dynamics of states and the composition of quantum systems.

Chapter 1

Introduction, Qubit and Single Qubit Gates

"Nature isn't classical, dammit, and if you want to make a simulation of Nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy."

The quote above is perhaps one of the most famous quotes in quantum computing and belongs to Richard Feynman [6]. In May 1981, while speaking about "Simulating physics with computers", he introduced the idea of a fundamentally new paradigm to build computing machines. Remarkably, he foresaw one of its most potent applications - "a simulation of Nature". Around the same time, Yuri Manin and Paul Benioff were also considering novel computation models based on quantum. Manin mainly focused on addressing the exponential cost of simulating many-particle systems with classical computers [7], while Benioff concentrated on whether a quantum computer could operate without dissipation [8].

In 1985, David Deutsch formalized the concept of a quantum computer [9]. Based on the previous work of Vazirani, Bernstein, and Simon, Peter Shor proposed in 1999 his famous quantum algorithm [10] that can solve the part of the factorization problem that proves to be very difficult for classical computers.

1999 is most probably a cornerstone moment for quantum computing and quantum communications. Suddenly, they jumped from exciting ideas to hot topics attracting the interest of researchers, commercial companies, and, last but not least, governments. Ever since, we've witnessed a sharp increase in interest, investments, and results. Still, more than four decades after Feynman's visionary statement, the problem of building and programming quantum devices "doesn't look so easy".

Throughout the years, we better understood the potential held by quantum computing and quantum communications. Besides security, chemistry and materials science are the most likely areas for quantum to succeed in the medium term. There is an increasing number of proposed approaches for machine learning as well, although the problems seem more difficult to tackle. Feynman's intuition was spot on. It proves to be quite difficult to build the physical devices and perhaps even more difficult to program them. Yet, when thinking of possibilities like provably

secure communications, efficient fertilizer production, mitigation of global warming through carbon capture, better batteries, lossless power lines, solvers for hard optimization problems - to name just a few - one cannot but be amazed by the potential lying ahead. Using quantum in computing and communications is the type of disruptive advancement that occurs maybe once in several generations.

Learning quantum computing and communications is not easy. Fortunately, there are people out there who are dedicating time and effort to make it as easier as possible. One of the most popular books is "Quantum Computation and Quantum Information" by Michael A. Nielsen and Isaac L. Chuang. If you are looking for a learning path that is more geared towards people with strong classical computing backgrounds, then "Quantum Computing for Computer Scientists" by Noson S. Yanofsky and Mirco. A. Mannucci is a better place to start. Similar to it, "Quantum Computer Science - An Introduction" by N. David Mermin is also an affordable place to start. If you fancy a (radically) different alternative, Bob Coecke's and Aleks Kissinger's "Picturing Quantum Processes - A First Course in Quantum Theory and Diagramatic Reasoning" is a memorable read.

There are many, many more materials, blogs, podcasts, and books out there. Hopefully, this material will also help you, the reader, advance into the amazing and spectacular fields of quamtum computing and communnications. Regardless where you start from, we encourage you to take the dive and prepare your mind to cope with a fundamental paradigm shift. It's going to be an incredible ride!

1.1 Single Qubit

1.1.1 Two-level quantum systems

Two-level quantum systems are ubiquitous in quantum mechanics and, among others, serve as the foundational building blocks for quantum computing in the form of qubits. These systems can exist in one of two basis states, often denoted as $|0\rangle$ and $|1\rangle$. In quantum mechanics, two-level systems manifest in various physical scenarios, such as the polarization of photons, the spin of spin-1/2 particles, and the energy levels of a two-level atom.

In quantum computing, all these two-state systems are abstracted into qubits. A **qubit** is the quantum analog of a classical bit and can exist in a superposition of its basis states $|0\rangle$ and $|1\rangle$. The general state of a qubit is given by a superposition of these basis states.

The mathematical formalism for qubits parallels that of these physical two-state systems, making them ideal candidates for physical implementations of quantum computing and communications.

For instance, the **polarization of light** can be described as a two-state system where the two basis states correspond to horizontal $|H\rangle$ and vertical $|V\rangle$ polarization.

In physics, quantum states can exist as **superposition** of other states. In particular, in quantum computing, qubits can exist in a superposition of states. For a qubit in a superposition represented by $|\psi\rangle$, its state can be written as:

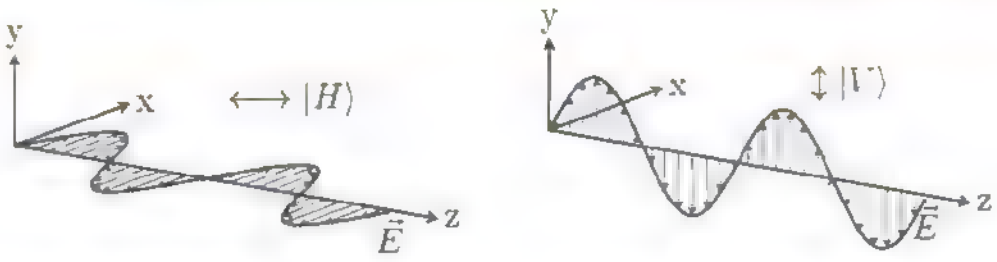


Fig. 1.1: (a) Horizontally polarized light; (b) Vertically polarized light (in both cases, only the electric field vector $\vec{E}$ is depicted, while the magnetic field vector $\vec{B}$, which is perpendicular on both the electric field one and the direction of propagation, $\vec{z}$ is omitted)

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

where α and β are related to the (probability) amplitudes for the states $|0\rangle$ and $|1\rangle$, respectively.

Superposition implies that the qubit (or system) is in both states $|0\rangle$ and $|1\rangle$ at the same time, but with different (complex) amplitudes. This leads one to consider linear algebra to study the problem, in the form of Dirac's bra-ket formalism.

1.1.2 The Bra-ket formalism

As seen in the previous chapter, bra-ket notation is a standard mathematical notation system used in quantum mechanics to describe quantum states and operations. It was introduced by Paul Adrien Maurice Dirac and, from a mathematical standpoint, is a concise way to represent vectors in Hilbert spaces, but from a physical point of view, it can denote the state of various physical systems. The notation consists of two types of elements: "bras" and "kets", therefore the physical "labels" discussed in the previous experimental situations are not just labels, they are mathematical vectors in the Hilbert state of a quantum system!

The appeal of this notation rests in its power to simplify the mathematical expressions in quantum mechanics and quantum computing, making it easier to manipulate and understand quantum states and operations.

A **ket** is represented by $|v\rangle$, where v is the label for the quantum state. It corresponds to a column vector in a Hilbert space. For example, in a two-level quantum system (qubit), the states can customarily be represented as follows

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

while a general ket can be represented as:

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix},$$

where α and β are complex numbers, not both simultaneously null. These two quantities are called the components of the ket $|\psi\rangle$ and can be also denoted by $\alpha = \psi_1, \quad \beta = \psi_2$

A **bra** is represented by $\langle\psi|$, where ψ is the label for the quantum state. It corresponds to a row vector in the dual Hilbert space. For example, the bras corresponding to the kets $\langle 0|$ and $\langle 1|$ are:

$$\langle 0| = \begin{pmatrix} 1 & 0 \end{pmatrix}, \quad \langle 1| = \begin{pmatrix} 0 & 1 \end{pmatrix}$$

while a general bra can be represented as

$$\langle\psi| = \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix}$$

where α and β are complex numbers, not both simultaneously null.

A bra is the Hermitian conjugate (complex conjugate transpose) of a ket and can be written as:

$$\langle\psi| = |\psi\rangle^\dagger = |\psi\rangle^{*T}$$

The **inner product** between two states $|\psi\rangle$ and $|\phi\rangle$ is denoted as $\langle\psi|\phi\rangle$. Mathematically, this is equivalent to the dot product for vectors. For two qubit states (of the same qubit), this takes the form:

$$\langle\psi|\phi\rangle = \psi_1^*\phi_1 + \psi_2^*\phi_2$$

The **outer product** between the states $|\phi\rangle$ and $|\psi\rangle$ is denoted as $|\phi\rangle\langle\psi|$. This operation produces a matrix, which for qubit states is a 2×2 matrix.

$$|\phi\rangle\langle\psi| = |\phi\rangle \times \langle\psi| = \begin{pmatrix} \phi_1\psi_1^* & \phi_1\psi_2^* \\ \phi_2\psi_1^* & \phi_2\psi_2^* \end{pmatrix}$$

While the inner product and outer product are two completely different mathematical beasts, one can observe that the inner product is the trace of the outer product (the sum of the diagonal elements in the matrix representation). This relation can be written as follows.

$$\langle\psi|\phi\rangle = \mathrm{Tr}|\phi\rangle\langle\psi|$$

Normalization is a crucial concept in quantum mechanics and quantum computing, ultimately ensuring that the probabilities associated with all possible outcomes of a measurement sum to one. This is a fundamental requirement for any valid quantum state.

The **norm** of a quantum state $|\psi\rangle$ is the real number

$$\||\psi\rangle\| = \sqrt{\langle\psi|\psi\rangle}$$

A quantum state $|\psi\rangle$ is said to be **normalized quantum state** if its norm is equal to one.

$$\||\psi\rangle\| = 1$$

or in other words, its inner product with itself is equal to one.

$$\langle\psi|\psi\rangle = 1$$

In a superposition of states, the coefficients (or probability amplitudes) must be chosen such that the state is normalized. For a qubit in a superposition state $\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, the normalization condition becomes: $|\alpha|^2 + |\beta|^2 = 1$. A normalized vector is illustrated in Figure 1.2.

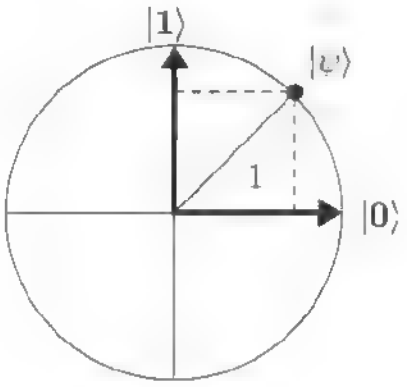


Fig. 1.2: Visual illustration of $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

Example. *Checking if a state is normalized.* Let us consider a qubit in the state $\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}\,1\rangle$. To check for normalization we have to compute:

$$|\alpha|^2 + |\beta|^2 = \left|\frac{1}{\sqrt{2}}\right|^2 + \left|\frac{i}{\sqrt{2}}\right|^2 = \frac{1}{2} + \frac{1}{2} = 1$$

As $|\alpha|^2 + |\beta|^2 = 1$, it follows that the state is normalized.

In quantum computing algorithms and operations. it is essential to ensure that states remain normalized after transformations. If a state becomes unnormalized due to some operation, it must be re-normalized by dividing each component by the norm.

$$|\psi\rangle_{\text{normalized}} = \frac{1}{\sqrt{\langle\psi|\psi\rangle}}|\psi\rangle$$

Example. *Normalizing a state.* Let us consider a qubit in the (unnormalized) state $|\psi\rangle = |0\rangle + |1\rangle$. To normalize it:

$$|\psi\rangle_{\text{normalized}} = \frac{1}{\sqrt{\langle\psi|\psi\rangle}}|\psi\rangle - \frac{1}{\sqrt{(\langle 0| - \langle 1\,)(|0\rangle + \langle 1\,)}}(|0\rangle + |1\rangle) =$$

$$= \frac{1}{\sqrt{\langle 0|0\rangle + \langle 1|1\rangle}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

The state is now normalized.

1.2 Bloch sphere representation

Normalization ensures that the quantum state is physically meaningful, as it guarantees that the sum of the probabilities of all possible outcomes is one. This is in line with the axioms of probability theory and is essential for the state to represent a real physical system. Therefore, normalization is not just a mathematical convenience but a fundamental aspect of quantum mechanics and quantum computing, ensuring the validity and physical feasibility of quantum states.

Considering a qubit in the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, let us assume that α and β have the following complex representation $\alpha = r_0 e^{i\varphi_0}$ and $\beta = r_1 e^{i\varphi_1}$, therefore:

$$|\psi\rangle = e^{i\varphi_0}(r_0|0\rangle + r_1 e^{i(\varphi_1-\varphi_0)}|1\rangle)$$

It can be proved that the factor $e^{i\varphi_0}$, corresponding to the overall phase of the state, is not observable. Therefore this factor can be discarded leading to:

$$|\psi\rangle = r_0|0\rangle + r_1 e^{i(\varphi_1-\varphi_0)}|1\rangle$$

Let us denote $\varphi = \varphi_1 - \varphi_0$, with $0 \leq \varphi < 2\pi$. Since $r_0|^2 + |r_1|^2 = 1$ we could interpret that $r_0 = \cos(\theta/2)$ and $r_1 = \sin(\theta/2)$, with $0 \leq \theta \leq \pi$.

Accordingly, a single qubit $|\psi\rangle$ can be expressed, in what is called the **Bloch sphere representation of a qubit**.

$$|\psi\rangle = \cos(\theta/2)\,|0\rangle + \sin(\theta/2)\,e^{i\varphi}\,|1\rangle \tag{1.1}$$

where θ is an angle (a real number between 0 and π) and φ is a phase (also a real number between 0 and 2π). The **Bloch sphere** is a geometrical representation of the state space of a single qubit based on the two-parameter algebraic representation relation (Equation 1.1), where, θ and φ are real numbers representing the polar and azimuthal angles, respectively, and therefore define a point on the surface of a unit sphere in 3D space. The north pole of the Bloch sphere corresponds to the state $|0\rangle$, and the south pole corresponds to the state $|1\rangle$, as is presented in Figure 1.3.

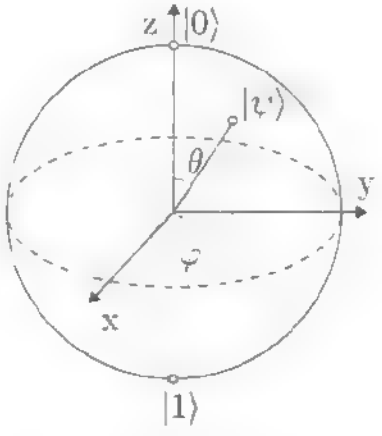


Fig. 1.3: Bloch sphere with the states $|0\rangle$, $|1\rangle$ and an arbitrary state $|\psi\rangle$

The Bloch sphere is particularly useful because it provides an intuitive way to visualize qubit states and the transformations that act upon them, such as quantum gates. It's important to note that this representation is specific to single qubits; for systems with more qubits, the state space becomes too complex to be easily visualized in this manner.

1.3 Bases, operators and measurements

1.3.1 Bases

In mathematics and quantum mechanics, a **discrete basis** refers to a set of linearly independent vectors that span a vector space, where the basis set itself is countable. As such, any vector in the space can be represented as a finite linear combination of the basis vectors, and the basis set is either finite or countably infinite.

A discrete basis $\{|e_i\rangle\}$ for the Hilbert space of a qubit has two elements, thus any vector $|\psi\rangle$ in the space can be uniquely represented as a superposition of two states.

$$|\psi\rangle = c_1|e_1\rangle + c_2|e_2\rangle$$

The vectors in a discrete basis are usually chosen to be orthonormal, meaning they are orthogonal and normalized.

$$\langle e_i|e_j\rangle = \delta_{ij}$$

where δ_{ij} is the Kronecker delta, which is 1 if $i = j$ and 0 otherwise. This means, that for the two elements of the **orthonormal basis** satisfy:

$$\langle e_1|e_2\rangle = \langle e_2|e_1\rangle = 0, \quad \langle e_1|e_1\rangle = \langle e_2|e_2\rangle = 1$$

For one qubit, the **computational basis** $\{|0\rangle, |1\rangle\}$ is a discrete basis having two elements. It is also an orthonormal basis, as $\langle 0\,0\rangle = \langle 1|1\rangle = 1$ and $\langle 0|1\rangle = \langle 1|0\rangle = 0$. The components of the state vector in this basis are $c_1 = \alpha$ and $c_2 = \beta$. This is in fact, the basis considered implicitly at the start of subsection 1.1.2. However, it ultimately is just one of multiple choices.

The **Hadamard basis** is another set of orthonormal vectors that can be used to describe qubit states, just like the computational basis states $|0\rangle$ and $|1\rangle$. The Hadamard basis is usually denoted by $\{|+\rangle, |-\rangle\}$, and its states are defined as follows.

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

The Hadamard basis serves as an alternative basis in which one can represent and manipulate quantum states, and it plays a crucial role in many quantum computing

and communication protocols. It will turn out later on to be particularly useful for creating superpositions and for tasks like quantum key distribution and quantum algorithms such as Grover's and the quantum Fourier transform.

Example. *Conversion from the standard computational basis to the Hadamard basis.* Let us consider $|\psi\rangle = \alpha\,0\rangle + 3|1\rangle$. To obtain the representation of $|\psi\rangle$ in the Hadamard basis we have to compute $\langle +|\psi\rangle$ and $\langle -|\psi\rangle$, as follows.

$$\langle +|\psi\rangle = \langle +|(\alpha|0\rangle + \beta|1\rangle) = \alpha\langle +|0\rangle + \beta\langle +|1\rangle = \frac{\alpha+\beta}{\sqrt{2}}$$
$$\langle -|\psi\rangle = \langle -|(\alpha|0\rangle + \beta|1\rangle) = \alpha\langle -|0\rangle + \beta\langle -|1\rangle = \frac{\alpha-\beta}{\sqrt{2}}$$

Therefore the representation of $|\psi\rangle$ in the Hadamard basis is:

$$|\psi\rangle = \left(\frac{\alpha+\beta}{\sqrt{2}}\right)|+\rangle + \left(\frac{\alpha-\beta}{\sqrt{2}}\right)|-\rangle$$

Equivalent descriptions of $|\psi\rangle$ are:

$$|\psi\rangle = \langle +|\psi\rangle|+\rangle + \langle -|\psi\rangle|-\rangle$$
$$|\psi\rangle = |+\rangle\langle +|\psi\rangle + |-\rangle\langle -|\psi\rangle$$
$$|\psi\rangle = (|+\rangle\langle +| + |-\rangle\langle -|)|\psi\rangle$$

which lead to the remark that $I = |+\rangle\langle +| + |-\rangle\langle -|$ is the identity operator. Similarly, the identity operator can be expressed using the computational basis $I = |0\rangle\langle 0| + |1\rangle\langle 1|$.

1.3.2 Operators

In quantum mechanics and quantum computing, operators act on states or qubit states to produce new states or to yield eigenvalues that can be measured.

An operator O is a **linear operator**, if for any two states $|\psi\rangle$ and $|\phi\rangle$ and complex scalars a and b, the operator O satisfies the condition

$$O(a|\psi\rangle + b|\phi\rangle) = aO|\psi\rangle + bO|\phi\rangle$$

An operator H is a **hermitian operator**, if it is equal to its hermitian conjugate.

$$H = H^\dagger$$

An operator U is a **unitary operator** if it satisfies the condition

$$U^\dagger U = UU^\dagger = I$$

Or, in other words, its inverse is also its Hermitian conjugate.

$$U^{-1} = U^{\dagger}$$

The **identity operator** I leaves the state unchanged and is represented by the 2x2 identity matrix:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

The Pauli matrices (corresponding to the **Pauli operators**) are a set of three 2x2 matrices, which have the following matrix representation.

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

The Pauli matrices exhibit several important mathematical and physical properties that make them useful in quantum mechanics and quantum computing.

- The trace of each Pauli matrix is zero: $\mathrm{Tr}(\sigma_x) = \mathrm{Tr}(\sigma_y) = \mathrm{Tr}(\sigma_z) = 0$
- The determinant of each Pauli matrix is -1: $\mathrm{Det}(\sigma_x) = \mathrm{Det}(\sigma_y) = \mathrm{Det}(\sigma_z) = -1$
- Each Pauli matrix is hermitian, being equal to its hermitian conjugate: $\sigma_x^{\dagger} = \sigma_x, \quad \sigma_y^{\dagger} = \sigma_y, \quad \sigma_z^{\dagger} = \sigma_z$
- Each Pauli matrix is unitary, meaning its inverse is its Hermitian conjugate: $\sigma_x\sigma_x^{\dagger} = I, \quad \sigma_y\sigma_y^{\dagger} = I, \quad \sigma_z\sigma_z^{\dagger} = I$
- The corresponding eigenvectors are the basis states for the qubit (for example $|0\rangle$ and $|1\rangle$ is an eigenvector for σ_z).
- Each Pauli matrix squared yields the identity matrix: $\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = I$
- While the Pauli matrices do not commute, they satisfy specific commutation and anti-commutation relations: $[\sigma_i, \sigma_j] = 2i\epsilon_{ijk}\sigma_k$, $\{\sigma_i, \sigma_j\} = 2\delta_{ij}I$ where $[\cdot,\cdot]$ denotes the commutator $[X, Y] = XY - YX$, $\{\cdot,\cdot\}$ denotes the anti-commutator $\{X, Y\} = XY - YX$, and ϵ_{ijk} is the Levi-Civita symbol, which takes the value 1 if the indices are in a natural order (1, 2, 3 or 2, 3, 1 or 3, 1, 2), the value -1 if they are i a mixed-up order (1, 3, 2 or 3, 2, 1 or 2, 1, 3), or 0 otherwise (for example if at least two indices are repeated).

In the context of quantum mechanics, the Pauli matrices correspond to the spin observables for spin-$\frac{1}{2}$ particles like electrons - σ_x, σ_y, and σ_z correspond to measurements of the spin along the x, y, and z axes, respectively. In quantum computing, the Pauli matrices are directly related to some of the most basic quantum gates. For example, the Pauli X matrix is essentially the NOT gate for qubits, while the Pauli Z gate applies a phase flip. These gates will turn out to be fundamental

building blocks for quantum algorithms. The Pauli matrices can also be thought as generators of rotations in the Bloch sphere representation of qubit states.

The **Hadamard operator** creates superpositions and is represented by:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

The **phase shift operator** adds a phase φ to the $|1\rangle$ state and is represented by:

$$R_\varphi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}$$

Projection operators (projectors, or measurement operators) project a state onto a particular basis, and will be useful when discussing physical measurements. For example, the projectors corresponding to the computational basis take the form:

$$M_0 = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \; M_1 = |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

or, in general for a state $|\psi\rangle$: $M_\psi = |\psi\rangle\langle\psi|$

In addition to being useful for measurements, projectors can be used to prepare specific states from a superposition. For example, the projector $|0\rangle\langle 0|$ will project any state onto the $|0\rangle$ state.

Such operators have a number of properties, any projector being:

- Idempotency - applying the operator twice in a row has the same result as just once: $M_\psi^2 = M_\psi$

- Hermitian - any projection operator is hermitian, being equal to its hermitian conjugate: $M_\psi^\dagger = M_\psi$

- Positive semi-definite: $\langle o|M|o\rangle \geq 0$ for all $|o\rangle$ states in the state space.

The **resolution of identity** (ROI) is a relation that allows the expression of the identity operator in terms of a sum over basis states. In the context of qubits, this is particularly straightforward, due to the 2-dimensional nature of a qubit's state space. In particular, for the computational basis states $|0\rangle$ and $|1\rangle$, the resolution of the identity can be expressed as:

$$I = |0\rangle\langle 0| + |1\rangle\langle 1| = M_0 + M_1$$

Operators play a crucial role in quantum algorithms, quantum gates, and quantum measurements, serving as the building blocks for manipulating and observing qubit states. In quantum optics, operators serve similar roles as they do in quantum mechanics and quantum computing, correspond to components that change the properties of light, but they are often tailored to describe the properties of light and its interaction with matter

1.3.3 Measurements

In quantum systems, **measurement** serves as the mechanism for obtaining classical information from the quantum state. Contrary to classical systems that are definitively in one state or the other, quantum systems can exist in superpositions of multiple states. However, upon measurement, the system provides a specific outcome, leading to a **collapse of the quantum state** into one of the basis states. In particular, in quantum computation, measurement is the process by which we extract classical information from a quantum system. Unlike classical bits that are either 0 or 1, qubits exist in superpositions. When measured, however, they yield a definite outcome, and the state of the qubit collapses to one of the basis states.

A **probability amplitude** is a complex number associated with the likelihood of finding (after a measurement) a quantum system in a particular state. If $|\psi\rangle$ is a quantum state and $|\phi\rangle$ is one of the basis states, the probability amplitude of finding $|\psi\rangle$ in the state $|\phi\rangle$ is given by the inner product $\langle\phi|\psi\rangle$.

In quantum mechanics, the outcome of a measurement is probabilistic, and these probabilities are determined by the amplitude of the quantum state in a particular basis. Specifically, the probability of obtaining a certain measurement outcome is the square of the absolute value of the amplitude corresponding to that outcome.

Probability amplitudes also account for quantum interference, a phenomenon where the probabilities aren't simply additive. The amplitudes add together, and only then are the probabilities calculated, leading to constructive or destructive interference. Understanding probability amplitudes is essential for grasping the fundamentals of quantum mechanics and quantum computing, as they govern the behavior and manipulation of quantum states.

The **probability** P of observing the state $|\phi\rangle$ when the system is in the state $|\psi\rangle$ is the square of the magnitude of the probability amplitude:

$$P(\phi) = |\langle\phi|\psi\rangle|^2$$

The most common type of measurement in quantum computing is projective measurement. For a qubit in state $|\psi\rangle$, the probability of measuring it in state $|0\rangle$ or $|1\rangle$ in the computational basis is given by:

$$P(0) = |\langle 0|\psi\rangle|^2$$

$$P(1) = |\langle 1|\psi\rangle|^2$$

After the measurement, the qubit state collapses to the measured state, either $|0\rangle$ or $|1\rangle$.

Example. *Probability amplitude* For a qubit in the state $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle$, the probability of measuring the state $|0\rangle$ would be:

$$P(0) = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$$

Similarly, the probability of measuring the state $|1\rangle$ would be:

$$P(1) = \left|\frac{i}{\sqrt{2}}\right|^2 = \frac{1}{2}$$

1.4 Gates

It is explicitly stated that the progression of a quantum state can be elucidated within the context of quantum computation. Similar to how a classical computer is constructed using electrical circuits composed of wires and logic gates, a quantum computer is constructed using a quantum circuit consisting of wires and elementary quantum gates. These quantum gates are employed to transport and manipulate quantum information. In the following section, we will introduce a few basic quantum gates and provide examples of circuits that demonstrate their use.

1.4.1 Single Qubit Gates, NOT gate

Classical computer circuits are composed of wires and logic gates, with wires serving as conduits for information transmission within the circuit. Logic gates, on the other hand, manipulate this information, transforming it from one state to another. To illustrate this concept, consider classical single-bit logic gates. Among these gates, the only one exhibiting non-trivial behavior is the NOT gate. It operates based on a defined truth table, wherein 0 is transformed into 1, and 1 is transformed into 0. In other words, it exchanges the states of 0 and 1.

The natural question that it comes is "can we define an analogous quantum gate for qubits?" Imagine if there were a process that could transition the quantum state $|0\rangle$ to $|1\rangle$ and vice versa. Such a process would naturally be a promising candidate for a quantum counterpart of the classical NOT gate. However, merely specifying how the gate affects the states $|0\rangle$ and $|1\rangle$ does not provide insight into its impact on superpositions of these states, without further understanding of the properties of quantum gates.

In reality, we expect that the quantum NOT gate operates linearly. This means it transforms a state $\alpha|0\rangle + \beta|1\rangle$ into the corresponding state where the roles of $|0\rangle$ and $|1\rangle$ have been swapped: $\alpha|1\rangle + \beta|0\rangle$.

1.4.2 Matrix representation of gates

The linearity of quantum gates allows for the representation of quantum operators, including the NOT gate, using an algebraic matrix format. Let's consider defining a matrix X to represent the quantum NOT gate as follows:

$$X \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

If the quantum state $\alpha|0\rangle + \beta|1\rangle$ is written in vectorial notation as:

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

with α and β corresponding to the amplitudes for $|0\rangle$ and $|1\rangle$ respectively. then the quantum NOT gate can be represented as:

$$X \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}.$$

The operation of the NOT quantum gate consists on transforming the state $|0\rangle$ into the state corresponding to the first column of the matrix X, while the state $|1\rangle$ is transformed into the state corresponding to the second column of the matrix X.

Quantum gates acting on a single qubit can be represented by 2×2 matrices. However. there are certain constraints on the matrices that can be used as quantum gates. Recall the normalization condition. which requires that $|\alpha|^2 + |\beta|^2 = 1$ for a quantum state $\alpha|0\rangle + \beta|1\rangle$. The same condition must hold true for any quantum state $|\psi'\rangle = \alpha'|0\rangle + \beta'|1\rangle$ obtained after the gate has operated.

Thuse, the matrix representation for the gate must adhere to a specific requirement: the matrix U. which describes the single qubit gate. must be unitary. In other words. it must satisfy the condition $U^\dagger U = UU^\dagger = I$. where $U^\dagger$ denotes the *adjoint* (hermitian conjugate) of U (obtained by transposing and complex conjugating U), and I represents the identity matrix. In our case the NOT gate. it is unitary because $X^\dagger X = XX^\dagger = I$.

1.4.3 Hadamard gate

The unitarity constraint stands as the sole requirement for quantum gates. Therefore. any unitary matrix can serve as a valid specification for a quantum gate. This implies an intriguing implication: unlike the classical scenario where only one non-trivial single-bit gate. the NOT gate. exists. the quantum field presents numerous non-trivial single-qubit gates. Among them. a highly used one is the Hadamard (H) gate defined by the matrix:

$$H \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

that transforms $|0\rangle$ into $(|0\rangle + |1\rangle)/\sqrt{2}$ and $|1\rangle$ into $(|0\rangle$ - $,1\rangle)/\sqrt{2}$.

Through elementary algebraic computation. it becomes evident that H^2 equals the identity matrix (I). Consequently. when applying the Hadamard gate (H) twice to a quantum state, it results in no alteration.

Operation on Bloch Sphere

The Hadamard gate stands out as one of the most valuable quantum gates. and it's worthwhile to visualize how it operates using the Bloch sphere representation.

In this representation, it becomes evident that single-qubit gates correspond to rotations and reflections of the sphere.

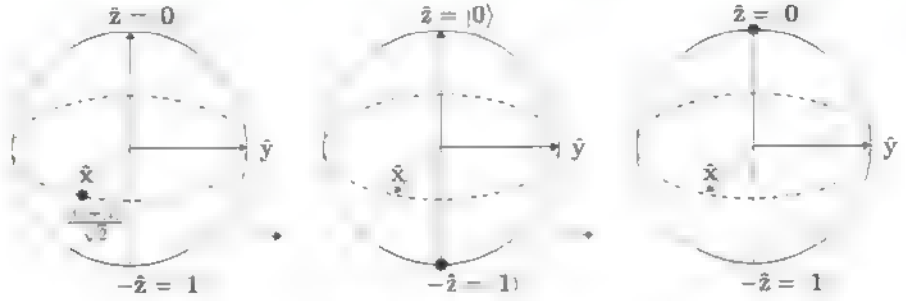


Fig. 1.4: Visual application of H gate on Bloch sphere

In Figure 1.4 the Hadamard operation can be described as a rotation of the quantum state sphere around the y-axis by 90 degrees, followed by a rotation around the x-axis by 180 degrees.

1.4.4 Unitary matrices, General single qubit gates

There exists an infinite number of 2×2 unitary matrices (see the section on unitary matrices in chapter 1), leading to an infinite variety of single-qubit gates. Nevertheless, it has been discovered that the characteristics of this entire set can be inferred by examining the properties of a smaller subset of them.

It can be proved that any 2×2 unitary matrix can be decomposed in a product of rotation matrices. More specifically, if U is a unitary matrix, then there exist four real values (α, β, γ and δ) such that U can be written as it is specified in Equation 1.2.

$$U = e^{i\alpha} \begin{pmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{pmatrix} \begin{pmatrix} \cos(\gamma/2) & -\sin(\gamma/2) \\ \sin(\gamma/2) & \cos(\gamma/2) \end{pmatrix} \begin{pmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{pmatrix} \quad (1.2)$$

The second matrix in the product is a standard rotation matrix, while the other two matrices correspond to rotations around the z axis. The $e^{i\alpha}$ factor corresponds to a phase shift. These matrices, being unitary, can be further decomposed leading to the possibility of obtaining a good approximation of arbitrary gates by using a finite set of gates which correspond to some fixed values of α, β, γ and δ.

1.4.5 Rotations, Pauli matrices, Phase gate, etc.

Pauli matrices are unitary matrices which define some common single qubit gates. There are three Pauli matrices, usually denoted as X, Y and Z and defined as in Equation 1.3.

$$X \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \quad Y \equiv \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}; \quad Z \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (1.3)$$

The name of Pauli matrices come from the fact that they perform rotations of π radians around the geometrical axis x, y and z. A general rotation of α radians around z axis it is also known as **phase shift gate**:

$$R_\alpha \equiv \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}, \forall \alpha \in \mathrm{R}$$

More specifically, it increases a qubit's relative phase by α:

$$R_\alpha = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix} \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) \\ e^{i\phi}\sin\left(\frac{\theta}{2}\right) \end{pmatrix} = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) \\ e^{i(\phi+\alpha)}\sin\left(\frac{\theta}{2}\right) \end{pmatrix} = \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right) e^{i\varphi}|1\rangle$$

Two other unitary matrices leading to single qubit gates are S (which corresponds to phase gate) and T (which corresponds to $\pi/8$ gate), described in the following.

$$S \equiv \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}; \qquad T \equiv \begin{pmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{pmatrix}$$

Fig. 1.5: Single bit logic gate

Unlike in the case of classical bits where there is just one gate transforming a bit (NOT - Figure 1.5), in the case of qubits there several important qubit gates (Figure 1.6).

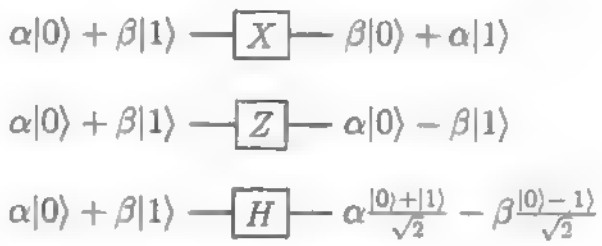


Fig. 1.6: Qubit logic gates

Properties of single qubit gates

These are several properties that illustrate the relationships among the above presented single-qubit gates:

$$\begin{aligned} HXH &= Z \\ HYH &= -Y \\ HZH &= X \\ TT &= S \\ TTTT &= Z \\ H &= (X+Z)/\sqrt{2} \end{aligned}$$

Chapter 2

Multiple Qubits and Universality

In classical computing, the complex operations arise from combinations of simple logic gates acting on multiple bits. Similarly, in quantum computing, it is the orchestrated interactions among multiple qubits, that enable us to perform non-trivial computations. In the following we delve into the intricacies of multi-qubit systems, exploring their properties and the fundamental role of universal quantum gates.

2.1 Systems with multiple qubits

2.1.1 Composite quantum systems

In this section we first present the formal method of representing systems that use the configuration of multiple qubits.

For example, in order to describe a system of two qubits, we can define it as follows:

$$\begin{cases} 00 \rightarrow |0\rangle|0\rangle = |00\rangle \\ 01 \rightarrow |0\rangle|1\rangle = |01\rangle \\ 10 \rightarrow |1\rangle|0\rangle = |10\rangle \\ 11 \rightarrow |1\rangle|1\rangle = |11\rangle \end{cases}$$

This can be seen as the quantum equivalent of the two bits combinations: 00, 01, 10 and 11. Therefor we can write the state of a two-qubit system as:

$$|\xi\rangle \equiv \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle, \tag{2.1}$$

where the sum of the squared norms of the amplitudes equals 1:

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1.$$

We can now define the basis states of a two-qubit system using the tensor product

as follows:

$$\begin{cases} |00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix}^T, \\ |01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \end{pmatrix}^T, \\ |10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \end{pmatrix}^T, \\ |11\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 \end{pmatrix}^T. \end{cases} \tag{2.2}$$

The representation of a superposition state using as a vector is $\begin{pmatrix} \alpha & \beta & \gamma & \delta \end{pmatrix}^T$.

The elements of $V_1 \otimes V_2 \otimes V_3 ... \otimes V_n$ are called n-qubits; they should be identified in correlation with the elements of $\mathbb{C}^2 \otimes \mathbb{C}^2 ... \otimes \mathbb{C}^2$.

Example. For $n = 2$, we assume that V_1 has a base of $\{|0\rangle_1, |1\rangle_1\}$, and V_2 has a base of $\{|0\rangle_2, |1\rangle_2\}$. The canonical basis of $V_1 \times V_2$ contains 4 elements $\{(|0\rangle_1, |0\rangle_2), (|0\rangle_1, |1\rangle_2), (|1\rangle_1, |0\rangle_2), (|1\rangle_1, |1\rangle_2)\}$, and the standard basis of $V_1 \otimes V_2$ is $\{(|0\rangle_1 \otimes |0\rangle_2), (|0\rangle_1 \otimes |1\rangle_2), (|1\rangle_1 \otimes |0\rangle_2), (|1\rangle_1 \otimes |1\rangle_2)\}$.

For $n = 3$, if V_i has the $\{|0\rangle_i, |1\rangle_i\}, 1 \leq i \leq 3\}$ base, then the standard basis of $V_1 \otimes V_2 \otimes V_3$ has $2^3 = 8$ tensors:

$$|0\rangle_1 \otimes |0\rangle_2 \otimes |0\rangle_3, |0\rangle_1 \otimes |0\rangle_2 \otimes |1\rangle_3, ..., |1\rangle_1 \otimes |1\rangle_2 \otimes |1\rangle_3,$$

or written in a more compact manner: $|000\rangle, |001\rangle, ..., |111\rangle$; we can also express these tensors as $|0\rangle, |1\rangle, ..., |7\rangle$, if we interpret the qubit values as numbers written in binary.

2.1.2 Space membership of qubits

There are multiple methods to create and interpret a system composed of two qubits:

- Both qubits can belong to the same party (they are local), being involved in the described protocol; for example, we can write the equivalent forms as follows:
  - $\alpha|0\rangle \otimes |0\rangle + \beta|0\rangle \otimes |1\rangle + \gamma|1\rangle \otimes |0\rangle + \delta|1\rangle \otimes |1\rangle$;
  - $\alpha|0\rangle|0\rangle + \beta|0\rangle|1\rangle + \gamma|1\rangle|0\rangle + \delta|1\rangle|1\rangle$;
  - $\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$;
- The qubits can belong to two different parties (spatially separated), that share the two qubit state, as presented in the following equivalent expressions:

- $\alpha|0\rangle_A \otimes |0\rangle_B + \beta|0\rangle_A \otimes |1\rangle_B + \gamma|1\rangle_A \otimes |0\rangle_B + \delta|1\rangle_A \otimes |1\rangle_B$;
- $\alpha|0\rangle_A|0\rangle_B + \beta|0\rangle_A|1\rangle_B + \gamma|1\rangle_A|0\rangle_B + \delta|1\rangle_A|1\rangle_B$;
- $\alpha|00\rangle_{AB} + \beta|01\rangle_{AB} + \gamma|10\rangle_{AB} + \delta|11\rangle_{AB}$.

2.1.3 Circuits for multiple qubits system

In order to define the circuits for multiple qubit systems, we should first interpret them mathematically, using the matrix form. We can therefor extend the tensor product operation to matrices as follows:

$$A \otimes B \equiv \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \otimes \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \equiv \begin{pmatrix} a_{11}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} & a_{12}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \\ a_{21}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} & a_{22}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \end{pmatrix}$$

$$\equiv \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{pmatrix}.$$

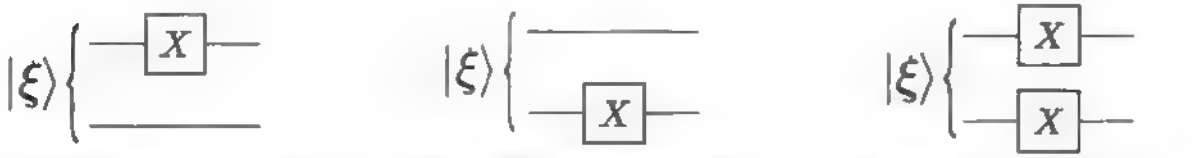
Example. We can now analyze how to express the action of the tensor product on multiple qubit systems. Some examples that involve using the NOT gate are illustrated in the circuits represented in Figure 2.1.

Starting from a general state ξ, defined using the notation from Equation 2.1, where:

$$|\xi\rangle \equiv \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle,$$

the action of the NOT gate in a multi qubit system changes the current state as follows:

- In Figure 2.1.a: $\alpha|10\rangle + \beta|11\rangle + \gamma|00\rangle + \delta|01\rangle$;
- In Figure 2.1.b: $\alpha|01\rangle + \beta|00\rangle + \gamma|11\rangle + \delta|10\rangle$;
- In Figure 2.1.c: $\alpha|11\rangle + \beta|10\rangle + \gamma|01\rangle + \delta|00\rangle$.



(a) A NOT gate applied on the first qubit.

(b) A NOT gate applied on the second qubit.

(c) NOT gates applied on both qubits.

Fig. 2.1: Systems with multiple qubits.

How can we formally describe the action of this gate on a single qubit, knowing that it is part of a system with more qubits?

The answer is to use to identity gate (I), alongside the NOT (X) gate, where both gates are 2×2 matrices applied to a single qubit. So, the effect of the NOT gate, as part of the circuits described in Figure 2.1, where the upper qubit has index 1, and the lower one has index 2, is as follows:

- In Figure 2.1.a: $X_1 I_2$;
- In Figure 2.1.b: $I_1 X_2$;
- In Figure 2.1.c: $X_1 X_2$.

Using the matrix form and the formal notations above, this can be explained as (for the first scenario):

$$\begin{pmatrix} \langle 00|X_1 I_2|00\rangle & \langle 00|X_1 I_2|01\rangle & \langle 00|X_1 I_2\ 10\rangle & \langle 00|X_1 I_2|11\rangle \\ \langle 01|X_1 I_2|00\rangle & \langle 01|X_1 I_2|01\rangle & \langle 01|X_1 I_2|10\rangle & \langle 01|X_1 I_2|11\rangle \\ \langle 10|X_1 I_2|00\rangle & \langle 10|X_1 I_2|01\rangle & \langle 10|X_1 I_2|10\rangle & \langle 10|X_1 I_2|11\rangle \\ \langle 11|X_1 I_2|00\rangle & \langle 11|X_1 I_2|01\rangle & \langle 11|X_1 I_2\ 10\rangle & \langle 11|X_1 I_2|11\rangle \end{pmatrix} = \\ = \begin{pmatrix} \langle 00|10\rangle & \langle 00|11\rangle & \langle 00|00\rangle & \langle 00|01\rangle \\ \langle 01|10\rangle & \langle 01|11\rangle & \langle 01|00\rangle & \langle 01|01\rangle \\ \langle 10|10\rangle & \langle 10|11\rangle & \langle 10|00\rangle & \langle 10|01\rangle \\ \langle 11|10\rangle & \langle 11|11\rangle & \langle 11|00\rangle & \langle 11|01\rangle \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}. \tag{2.3}$$

The result from Equation 2.3 can also be obtained by combining the two matrices (X and I) into a single one, that acts on the vector state describing the whole system; for two qubits, the possible combinations are detailed in the set of Equations 2.2. The equivalent transformation for the first scenario is presented in the following equation:

$$X \otimes I = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

We can similarly find the matrix forms for the scenarios in Figures 2.1.b ($I \otimes X$) and 2.1.c ($X \otimes X$).

2.1.4 Probability amplitudes for composite systems

Up until this point we analyzed the probability amplitude of a single qubit system, using the braket notation. We can write $\langle 0|1\rangle$ to indicate the probability amplitude for the quantum state $|1\rangle$ of being in state $|0\rangle$.

For example, let us examine the following four quantum single-qubit states $|\phi_0\rangle$, $|\phi_1\rangle$, $|\psi_0\rangle$ and $|\psi_1\rangle$. They can be combined to generate the following two-qubit quantum states: $|\phi_0\rangle \otimes |\psi_0\rangle$, $|\phi_1\rangle \otimes |\psi_1\rangle$ or $|\phi_0, \psi_0\rangle$, $|\phi_1, \psi_1\rangle$.

We can express the probability of one composite state in a similar manner to the described single qubit expression. The probability amplitude of having the $|\phi_0, \psi_0\rangle$ state in the $|\phi_1, \psi_1\rangle$ state is $\langle \phi_1, \psi_1 | \phi_0, \psi_0 \rangle$,

which can be further calculated as the multiplication of brakets for each qubit: $\langle \phi_1, \psi_1 | \phi_0, \psi_0 \rangle = \langle \phi_1 | \phi_0 \rangle \langle \psi_1 | \psi_0 \rangle$.

2.1.5 Multiple qubit gates

The gates that act on multiple qubits play a crucial role in the quantum algorithms that have been proposed over the years. They make possible the implementation of concepts such as entanglement (that will be discussed later), and therefor more complex protocols.

In this section we present the most relevant multiple qubit gates.

The CNOT gate

The controlled-NOT gate (or the short version, $CNOT$) acts on two qubits, where one of them is called the control qubit, and the other one is the target qubit. Its effect can be described with two simple statements:

- If the control qubit ($|q_c\rangle$) is in the $|0\rangle$ state, then the target qubit ($|q_t\rangle$) remains unchanged;
- If the control qubit ($|q_c\rangle$) is in the $|1\rangle$ state, then the state of the target qubit ($|q_t\rangle$) is inverted.

The CNOT gate is shown in Figure 2.2.

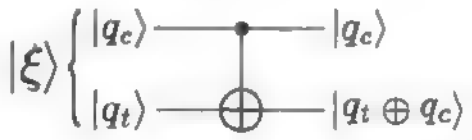


Fig. 2.2: The representation of the CNOT gate.

The effect of this quantum gate is also summarized can be summarized as follows. Applied upon the $|00\rangle$ and $|11\rangle$ states, the CNOT gate has no effect. However, CNOT applied to $|01\rangle$ turns it into $|10\rangle$, and $|10\rangle$ is turned to $|01\rangle$.

The formal action of applying the CNOT gate to a generic two qubit state can be expressed as:

$$\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \xrightarrow{CNOT} \alpha|00\rangle + \beta|01\rangle + \gamma|11\rangle + \delta|10\rangle.$$

The CNOT gate has the following equivalent matrix form.

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

The CNOT gate is actually an instance of a more general class of gates, the *controlled-U* gates. The U operator is applied on the target qubit only if the control qubit is in the $|1\rangle$ state. If the control qubit is in the $|0\rangle$ state, then the U operator plays the role of the I gate. This can be formally written as follows:

$$C_U = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U.$$

Figure 2.3 illustrates a controlled-U gate.

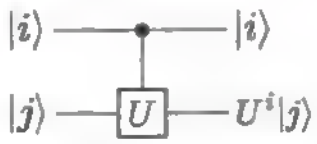


Fig. 2.3: The representation of the general controlled-U gate

This action can also be expressed as:

$$C_U \equiv I \otimes U^i,$$
$$C_U|i\rangle|j\rangle = |i\rangle\, U^i\, |j\rangle,\ i,j \in \{0,1\}.$$

Using the introduced notations, we can now draw the conclusion that the CNOT gate is actually the C_X gate, where the NOT gate play the role of the U operator. For the matrix representation we can write:

$$CNOT \equiv I \otimes X^i = \begin{pmatrix} I_2 & 0 \\ 0 & X \end{pmatrix}.$$

One property of the CNOT gate is that the transpose of the CNOT gate is the CNOT gate itself:

$$CNOT^T = CNOT.$$

In addition, the product of the CNOT matrix and its conjugate transpose ($CNOT^\dagger$ notation) leads to the identity matrix: this is true for all quantum gates, as they are represented by unitary matrices:

$$CNOT \cdot CNOT^\dagger = CNOT^\dagger \cdot CNOT = I_4.$$

We also notice that by applying the CNOT gate twice (in succession), we are in fact returning to the original system state, as:

$$CNOT \cdot CNOT = \begin{pmatrix} I_2 & 0 \\ 0 & X \end{pmatrix}\begin{pmatrix} I_2 & 0 \\ 0 & X \end{pmatrix} = \begin{pmatrix} I_2 & 0 \\ 0 & X^2 \end{pmatrix} = \begin{pmatrix} I_2 & 0 \\ 0 & I^2 \end{pmatrix} = I_4.$$

We can also write the formal effect of the CNOT gate, for the basis states $|i\rangle$ and $|j\rangle$, such that $CNOT|i\rangle|j\rangle = |i\rangle|j \oplus i\rangle$.

By applying the CNOT gate again, we can easily see that the output returns the initial state $CNOT|i\rangle|j \oplus i\rangle = |i\rangle|j \oplus i \oplus i\rangle = |i\rangle|j\rangle$.

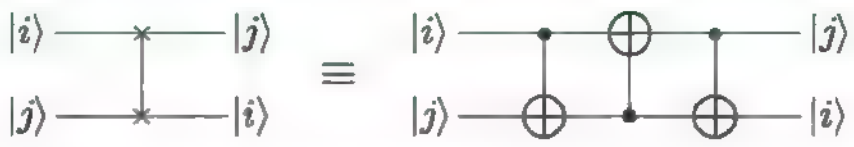


Fig. 2.4: The SWAP gate and the equivalent circuit, using three CNOT gates.

The SWAP gate

Another gate that acts on two qubits is the SWAP gate, which exchanges the state of its two input qubits. It can be obtained by applying three CNOT gates, as shown in Figure 2.4.

Let us now see the system state at each step of the equivalent circuit (after each CNOT gate):

- $CNOT|i\rangle|j\rangle = |i\rangle|j \oplus i\rangle$
- $CNOT|j \oplus i\rangle|i\rangle = |j \oplus i\rangle|i \oplus j \oplus i\rangle = |j \oplus i\rangle|j\rangle$
- $CNOT|j\rangle|j \oplus i\rangle = |j\rangle|j \oplus i \oplus j\rangle = |j\rangle|i\rangle$

As quantum gates have a linear operation on the inputs, superposition states will also be swapped. Assuming the following two general qubit states:

$$\begin{cases} |\psi\rangle = a|0\rangle + b|1\rangle \\ |\phi\rangle = c|0\rangle + d|1\rangle, \end{cases}$$

by applying the SWAP gate on the composite state, we obtain:

$$\begin{aligned} SWAP\,|\psi\rangle \otimes |\phi\rangle &= SWAP(ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle) \\ &= ac|00\rangle + ad|10\rangle + bc|01\rangle + bd|11\rangle \\ &= ca|00\rangle + cb|01\rangle + da|10\rangle + db|11\rangle \\ &= |\phi\rangle \otimes |\psi\rangle, \quad \forall\, |\psi\rangle, |\phi\rangle. \end{aligned}$$

Three-qubit controlled gates

We can extend the concepts discussed in the previous sections to create a three-qubit system in multiple ways.

One method is by adding an addtional control qubit: in this way, we basically design the *controlled-controlled-NOT* gate (CCNOT or Toffoli gate), as illustrated in Figure 2.5.

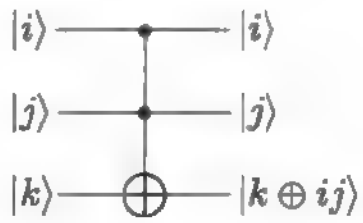


Fig. 2.5: The CCNOT (Toffoli) gate.

The two upper qubits, $|i\rangle$ and $|j\rangle$ are the control qubits, and the lower one, $|k\rangle$, is the target qubit. If both control qubits are in the $|1\rangle$ state, then the state of the target qubit is inverted; otherwise, it is left unchanged. This can be formally described as follows:

$$CCNOT|i\rangle|j\rangle|k\rangle = |i\rangle|j\rangle\ |k \oplus ij\rangle,$$

with $i, j, k \in \{0, 1\}^3$.

Another idea is to have a control qubit that allows a SWAP operation between two other qubits, hence, the *controlled-SWAP* gate (also called the CSWAP, or Fredkin gate), presented in Figure 2.6. If the control qubit is in the $|1\rangle$ state, only then the other two qubits are swapped, otherwise there is no change in their state.

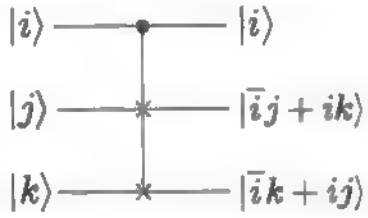


Fig. 2.6: The controlled-SWAP (Fredkin) gate.

The action of the Fredkin gate can be formally expressed as:

$$CSWAP|i\rangle|j\rangle|k\rangle = |i\rangle|\bar{i}j + ik\rangle|\bar{i}k + ij\rangle.$$

As they operate on three qubits, the mathematical action of these gates can be described using 8×8 matrices.

General n-qubit gates

A general quantum system, made of n qubits, can be described as follows:

$$|\Psi_n\rangle \equiv |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle, \tag{2.4}$$

where $|\psi_i\rangle = a_i|0\rangle + b_i|1\rangle$, for $i = \overline{1, n}$.

Using the U_i notation for the transformation effect on each qubit $|\psi_i\rangle$, with $i = \overline{1, n}$, the evolution of the system (by applying an n-qubit gate) can be expressed as:

$$\mathcal{U}_n \equiv U_1 \otimes U_2 \otimes \ldots U_n.$$

By applying this transformation to the system described in Equation 2.4, the state of the system can be further written as:

$$\begin{aligned}\mathcal{U}_n|\Psi_n\rangle &= (U_1 \otimes U_2 \otimes \ldots U_n)(|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle) \\ &= U_1|\psi_1\rangle \otimes U_2|\psi_2\rangle \otimes \cdots \otimes U_n|\psi_n\rangle.\end{aligned}$$

2.1.6 The Walsh-Hadamard Transform

The Hadamard gate can be extended to multiple qubit systems; this is known as *the Walsh-Hadamard transform*, and its formal recursive expression is:

$$H_n = H_1 \otimes H_{n-1}, \quad n \geq 1, \tag{2.5}$$

and

$$\begin{cases} H_0 \equiv 1, \\ H_1 \equiv H = \dfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \end{cases}$$

After expanding the expression in Equation 2.5, we obtain:

$$\begin{aligned} H_n &= H_1 \otimes H_{n-1} \\ &= H_1 \otimes H_1 \otimes H_{n-2} = \dots \\ &= \underbrace{H_1 \otimes H_1 \otimes \cdots \otimes H_1}_{\text{n times}} \\ &\equiv H_1^{\otimes n}. \end{aligned}$$

Example. We now present how to interpret the application of the Walsh-Hadamard transform on a two-qubit system, as presented in Figure 2.7. The initial state of the system is $|\xi\rangle = |00\rangle$.

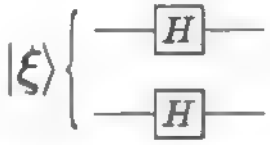


Fig. 2.7: The Walsh-Hadamard transform applied on a system of two qubits.

The formal action of the Walsh-Hadamard transform can be expressed as follows:

$$\begin{aligned} H_2|00\rangle &= (H_1 \otimes H_1)|00\rangle \\ &= H_1|0\rangle \otimes H_1|0\rangle \\ &= \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \\ &= \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}. \end{aligned}$$

If we apply this transform on an n-qubit system state, where each qubit is initially in the $|0\rangle$ state:

$$|\xi\rangle = \underbrace{|0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle}_{\text{n times}} \equiv |0\rangle^{\otimes n},$$

then we obtain the following:

$$H_n|0\rangle^{\otimes n} = H_1^{\otimes n}|0\rangle^{\otimes n} = (H_1|0\rangle)^{\otimes n} = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{k \in \{0,1\}^n} |k\rangle.$$

with $|k\rangle$ any computational basis state of the n dimensional space.

What is very important to notice is that by applying a set of Hadamard gates on a system initially set to the $|0\rangle^{\otimes n}$ state, the system is then configured to a **superposition of all the computational basis states**, all with an equal probability of $1/2^n$.

2.2 Universal gates

2.2.1 Measurement of systems with multiple qubits

As a reminder, if we express a general state of two qubits such that:

$$|\xi\rangle \equiv \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle,$$

then we know that $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$, and $\alpha = \langle 00|\xi\rangle$, $\beta = \langle 01|\xi\rangle$, $\gamma = \langle 10|\xi\rangle$, $\delta = \langle 11|\xi\rangle$

Using the following notations (projections operators):

$$\begin{cases} \Pi_{00} \equiv |00\rangle\langle 00|, \\ \Pi_{01} \equiv |01\rangle\langle 01|, \\ \Pi_{10} \equiv |10\rangle\langle 10|, \\ \Pi_{11} \equiv |11\rangle\langle 11|, \end{cases}$$

by applying the Born rule, we can write:

$$\begin{cases} \langle\xi|\Pi_{00}|\xi\rangle = |\alpha|^2, \\ \langle\xi|\Pi_{01}|\xi\rangle = |\beta|^2, \\ \langle\xi|\Pi_{10}|\xi\rangle = |\gamma|^2, \\ \langle\xi|\Pi_{11}|\xi\rangle = |\delta|^2. \end{cases}$$

2.2.2 Universal quantum gates

When it comes to the classical processing of information, we know that:

- any function can be implemented by using certain fundamental gates (only *AND* and *NOT* gates / *NAND* gates, or *OR* and *NOT* gates / *NOR* gates);
- more complicated gates can be designed only with the universal gates mentioned above.

In quantum computing, any unitary operation on n qubits can be implemented using the *CNOT* gate and single-qubit gates - they represent a universal set for the quantum computations (other sets also exist). Then a quantum computer can be built by using only *CNOT* and single-qubit gates.

Quantum computing operates on principles distinctly different from classical computing, though it shares the foundational concept of processing information through a structured arrangement, akin to a circuit formed of gates. This arrangement, known as the quantum circuit model, processes inputs and incorporates measurement devices to statistically analyze the resulting outputs. The entire quantum computation process unfolds in a structured manner, which can be conceptually segmented into three stages.

First, we define our initial conditions by setting up the initial state. This is typically represented by a computational basis state, which serves as the quantum analogue to classical bits in traditional computing. This state acts as the foundation upon which subsequent quantum operations are applied.

The second stage involves the application of quantum gates. Each gate performs a specific operation, altering the qubit's state or creating intricate relationships between qubits. The sequence and combination of these gates define the computational logic of the quantum algorithm.

Finally, after the gates have been applied, we get to the third and final stage: measurement. Through measurement, we effectively collapse these superpositions into definite states, obtaining the result of our quantum computation.

2.2.3 The no-cloning theorem

In classical computing we can easily copy a bit by using a CNOT gate: the input value (x) is connected to the control bit, and a bit with value 0 is connected to act as the target bit. In this way, both output bits will hold the x value.

Assuming we would try to use the same idea with the quantum CNOT gate, for a qubit that is in the following state:

$$|\psi\rangle = a|0\rangle + b|1\rangle,$$

then the system can be formally described as follows (the target qubit is set to $|0\rangle$ in this scenario, see Figure 2.8):

$$\begin{aligned} CNOT(|\psi\rangle, |0\rangle) &= CNOT(a|0\rangle + b|1\rangle, |0\rangle) = a\, CNOT(|00\rangle) + b\, CNOT(|10\rangle) \\ &= a|00\rangle + b|11\rangle. \end{aligned}$$

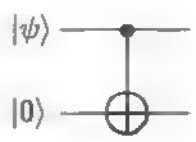


Fig. 2.8: Trying to copy a quantum state using a CNOT gate.

Only if $|\psi\rangle = |0\rangle (a = 1 \text{ and } b = 0)$ or $|\psi\rangle = |1\rangle (a = 0 \text{ and } b = 1)$, we manage to copy the state.

Otherwise, **for the general scenario**, the result is as follows:

$$|\psi\rangle|\psi\rangle = (a|0\rangle + b|1\rangle)(a|0\rangle + b|1\rangle) = a^2|00\rangle + ab|01\rangle + ab|10\rangle + b^2|11\rangle.$$

Except for the case where $ab = 0$, **it is impossible to create a copy or clone of an unknown quantum state** (this is known as the no-cloning theorem), theorized in 1982 by Wootters and Zurek.

2.2.4 The Superdense Coding protocol

So we have two parties Alice and Bob which are far away one from each other. Their goal is to send some classical information from Alice to Bob. Alice has 2 bits of information that she needs to sent to Bob but she can only transmit to Bob a single qubit. We can see the procedure that Alice and Bob can apply in Figure 2.9.

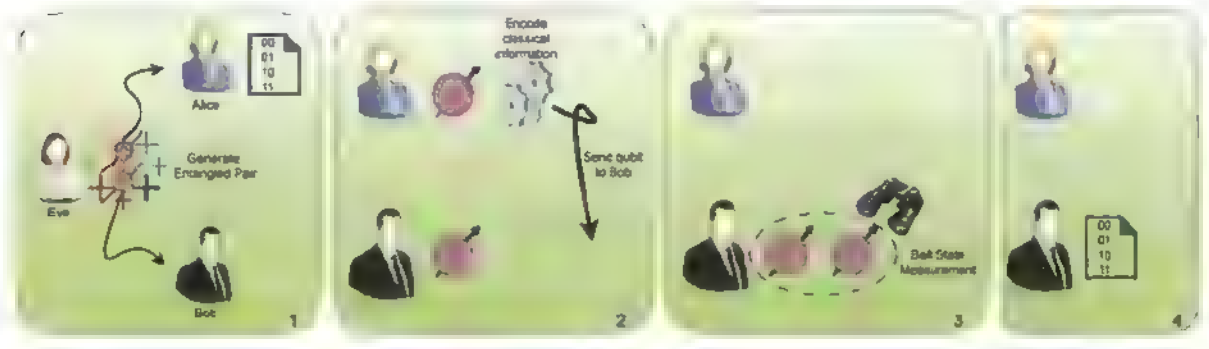


Fig. 2.9: The Superdense Coding protocol.

We have to consider that Alice and Bob share a both a single qubit from an entangled state, that was somehow produced by a third party, Eve. In the Superdense Coding algorithm circuit presented in Figure 2.11, we would be in the $T1$ moment. Once Alice and Bob each receive their qubit, Alice can begin the preparation of encoding two classical bits in her qubit. If the two classical bits that she has are 00, she does nothing to the qubit, if she has 01, then she uses the X gate, for 10 she uses the Z gate, and if both classical bits are 1, she applies the ZX gates, then she sends her qubit to Bob. This is the $T2$ moment in Figure 2.11. We can observe the results of Alice's operations in Figure 2.10.

Alice's message	Gate(s)	$\|\psi_2\rangle$	$\|\psi_3\rangle$	$\|\psi_4\rangle$
00	I	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|10\rangle)$	$\|00\rangle$
01	X	$\frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$	$\frac{1}{\sqrt{2}}(\|11\rangle + \|01\rangle)$	$\|01\rangle$
10	Z	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|10\rangle)$	$\|10\rangle$
11	ZX	$\frac{1}{\sqrt{2}}(-\|10\rangle + \|01\rangle)$	$\frac{1}{\sqrt{2}}(-\|11\rangle + \|01\rangle)$	$\|11\rangle$

Fig. 2.10: The states from the Superdense Coding circuit.

Now that Bob has both qubits he will perform the inverse operation Eve that has done, i.e. applying a CNOT gate and a H gate for the first qubit in order to perform a Bell State Measurement. Through the measurement. he gets exactly the 2 bits of information sent by Alice, at moment $T3$ of Figure 2.11. This is the superdense coding protocol, first proposed by Charles H. Bennett and Stephen Wiesner in 1970.

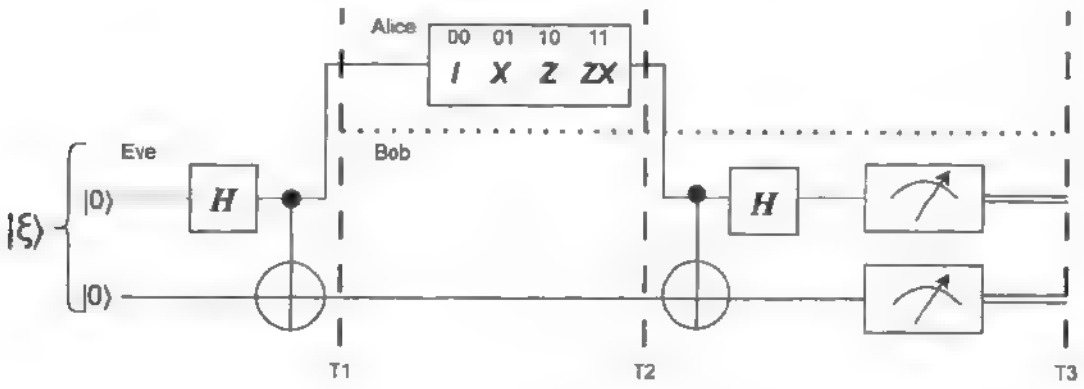


Fig. 2.11: The Superdense Coding algorithm circuit.

Chapter 3

Entanglement and Quantum Teleportation

"Spooky action at a distance." - Albert Einstein

Albert Einstein's description of quantum entanglement encapsulates the non-intuitive, non-local properties of quantum systems. Entanglement, a cornerstone of quantum mechanics, defies our classical intuition by allowing particles to become so deeply intertwined that the state of one instantaneously affects the state of another, regardless of the distance separating them. This phenomenon, though once a subject of philosophical debates and skepticism, today stands not only as a fundamental pillar of quantum theory but also as a crucial resource for emerging quantum technologies.

In this chapter we will uncover one of the most captivating applications of entanglement: quantum teleportation. Quantum teleportation is a process through which the state of a quantum system can be transmitted from one location to another with the help of two entangled particles and classical communication. Make no mistake, we are not talking about the science fiction trope of teleporting matter here. The process of quantum teleportation offers a genuine solution solely for transmitting quantum *information* across vast distances, overcoming classical limitations.

3.1 Entanglement

Let us consider a two-qubit system whose Hilbert space is denoted by $\mathcal{H}_A \otimes \mathcal{H}_B$.

Definition 3.1. *If the state of two qubits can be written as a product state*

$$|\psi\rangle_{AB} = |\xi\rangle_A \otimes |\eta\rangle_B.$$

then the state is called **separable** *or* **product**. *The two states $|\xi\rangle$ and $|\eta\rangle$ are arbitrary states of a qubit.*

Definition 3.2. *If the state of two qubits cannot be written as a product state, i.e.*

$$|\psi\rangle_{AB} \neq |\phi\rangle_A \otimes |\chi\rangle_B,$$

then the state is called **entangled.**

Erwin Schrödinger noted the existence of entanglement in 1935 (Verschränkung in German) between parts of a multiparticle quantum system. It can be described as a kind of correlations between two or more subsystems.

As an example of entanglement, let us consider the following state of two qubits:

$$|\beta_{00}\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B). \tag{3.1}$$

The fact that this state is entangled can be easily checked by taking the qubit states

$$\begin{aligned} |\xi\rangle_A &= \alpha_A|0\rangle + \beta_A|1\rangle, \\ |\eta\rangle_B &= \alpha_B|0\rangle + \beta_B|1\rangle, \end{aligned}$$

where α_j and β_j (with $j = A, B$) are non-vanishing complex parameters. Suppose that there are α_j and β_j such that $|\beta_{00}\rangle_{AB} = |\xi\rangle_A|\eta\rangle_B$. We build the product state

$$|\xi\rangle_A\,\eta\rangle_B = \alpha_A\alpha_B|00\rangle - \alpha_A\beta_B|01\rangle + \beta_A\alpha_B|10\rangle + \beta_A\beta_B|11\rangle. \tag{3.2}$$

By making a comparison between Eqs. (3.1) and (3.2), we find that there is no solution to the problem, since all the four parameters α_A, α_B, β_A, and β_B are non-zero. This leads to the conclusion that the state (3.1) is entangled.

3.2 Partial measurement in quantum mechanics

The postulate of quantum measurement was discussed in Chapter 1 in the case of a single-system. Consider now a quantum system composed of two subsystems, denoted by A and B. We want to measure only an observable associated to the first subsystem A, while doing nothing to the second subsystem; this kind of measurement is called **partial measurement.**

Let us discuss the case of two qubits. The general state of this system is:

$$|\Psi\rangle_{AB} = \alpha|0\rangle_A|0\rangle_B + \beta|0\rangle_A|1\rangle_B + \gamma|1\rangle_A|0\rangle_B + \delta|1\rangle_A|1\rangle_B,$$

where α, β, γ, and δ are complex parameters, satisfying the normalization condition

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1.$$

Suppose that we perform a measurement on the system A only. The probability of obtaining the outcome "0" is:

$$p_0 = |\alpha|^2 + |\beta|^2,$$

and the final state is

$$|\phi_0\rangle = \frac{1}{p_0}(\alpha|0\rangle_A|0\rangle_B + \beta|0\rangle_A|1\rangle_B).$$

On the other hand, the probability of obtaining the outcome "1" is:

$$p_1 = |\gamma|^2 + |\delta|^2,$$

while the final state is

$$|\phi_1\rangle = \frac{1}{p_1}(\gamma|1\rangle_A|0\rangle_B + \delta|1\rangle_A|1\rangle_B).$$

This discussion can easily be extended to the case of multiparticle systems.

3.3 Generation of the Bell states

The state of Equation (3.1) belongs to the set of the so-called Bell states defined as follows:

$$\begin{aligned}
|\beta_{00}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \\
|\beta_{01}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \\
|\beta_{10}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \\
|\beta_{11}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).
\end{aligned}$$

All the four Bell states are entangled.

The Bell states can be generated by using the quantum circuit shown in Fig. 3.1. In all the four cases the input state is $|00\rangle$. The circuit consists of. the single-qubit gates U_1 and U_2. the Hadamard gate H, followed by the CNOT gate.

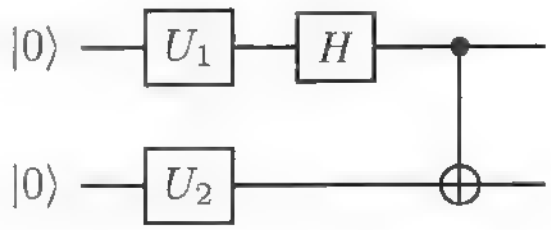


Fig. 3.1: The quantum circuit used for the generation of the Bell states.

a) For generating the state $|\beta_{00}\rangle$, the unitary operators are $U_1 = I$ and $U_2 = I$:

$$|00\rangle \xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

and the final state is

$$|\phi_0\rangle = \frac{1}{p_0}(\alpha|0\rangle_A|0\rangle_B + \beta|0\rangle_A|1\rangle_B).$$

On the other hand, the probability of obtaining the outcome "1" is:

$$p_1 = |\gamma|^2 + |\delta|^2,$$

while the final state is

$$|\phi_1\rangle = \frac{1}{p_1}(\gamma|1\rangle_A|0\rangle_B + \delta|1\rangle_A|1\rangle_B).$$

This discussion can easily be extended to the case of multiparticle systems.

3.3 Generation of the Bell states

The state of Equation (3.1) belongs to the set of the so-called Bell states defined as follows:

$$\begin{aligned}
|\beta_{00}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \\
|\beta_{01}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \\
|\beta_{10}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \\
|\beta_{11}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).
\end{aligned}$$

All the four Bell states are entangled.

The Bell states can be generated by using the quantum circuit shown in Fig. 3.1. In all the four cases the input state is $|00\rangle$. The circuit consists of. the single-qubit gates U_1 and U_2. the Hadamard gate H, followed by the CNOT gate.

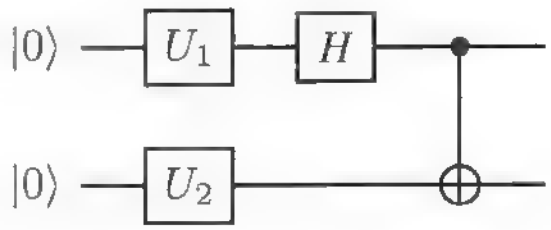


Fig. 3.1: The quantum circuit used for the generation of the Bell states.

a) For generating the state $|\beta_{00}\rangle$, the unitary operators are $U_1 = I$ and $U_2 = I$:

$$|00\rangle \xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

b) For generating the state $|\beta_{01}\rangle$, the unitary operators are $U_1 = I$ and $U_2 = X$:

$$|00\rangle \xrightarrow{I\otimes X} |01\rangle \xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle).$$

c) For generating the state $|\beta_{10}\rangle$, the unitary operators are $U_1 = X$ and $U_2 = I$:

$$|00\rangle \xrightarrow{X\otimes I} |10\rangle \xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle).$$

d) For generating the state $|\beta_{11}\rangle$, the unitary operators are $U_1 = X$ and $U_2 = X$:

$$|00\rangle \xrightarrow{X\otimes X} |11\rangle \xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}(|01\rangle - |11\rangle) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

3.4 The Einstein - Podolsky - Rosen paradox

In 1935, Einstein, Podolsky, and Rosen (EPR) published a paper called *"Can Quantum Mechanical description of reality be considered complete?"*, in which they argued about an apparent paradox that would prove that quantum mechanics is an incomplete theory.

In their definition, a *complete* theory was one where "*every element of the physical reality must have a counterpart in the physical theory.*" In which by "*physical reality*" they understood that "*If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity.*" In other words, one considers a theory, where the observables are characterized by definite values, which are independent on the measurement performed on the system: this concept is known as *realism*. In addition, the theory should be *local*, i.e. it is supposed that no action at the distance exists.

In this section we discuss the Bohm's argument about this topic, which is a simplified version of the initial proposal of Einstein, Podolsky, and Rosen. The Bohm-EPR Gedankenexperiment provides a simplification, since the measurements of spin operators on this system have only two possible outcomes, ± 1 in $\hbar/2$ units, and not a continuous range of outcomes, such as the position and the momentum in the example given by EPR. In the Bohm-EPR Gedankenexperiment, Alice and Bob receive from a source a pair of spin 1/2 particles described by the singlet state, which is the Bell state $|\beta_{11}\rangle$:

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle_A|\downarrow\rangle_B - |\downarrow\rangle_A|\uparrow\rangle_B) = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B).$$

Above we have used the notations: $|0\rangle = |\uparrow\rangle$ and $|1\rangle = |\downarrow\rangle$.

Alice performs a measurement of the spin of her particle along the Oz-axis, while Bob measures the spin of his particle along the Oz-axis.The assumptions of *reality* and *locality* would imply that the result of Alice's measurement will not affect the result of the Bob's measurement.

There are two possibilities:

a) Alice obtains spin "↑" with probability 1/2. In this case, Bob's outcome is "↓".

b) Alice obtains spin "↓" with probability 1/2, while Bob's outcome is "↑".

A measurement of the spin of one particle influences the outcome of the other particle. The conclusion is that quantum mechanics is a nonlocal theory. This paradox is known in the scientific literature as the **Einstein - Podolsky - Rosen (EPR) paradox**. It analyzes two important aspects of quantum mechanics, namely its probabilistic nature and the existence of non-locality.

3.5 The Bell inequality

The Bell inequality is a tool, which helped the physicists to invalidate the assumptions in the EPR paradox.

Consider an observer Charlie, who is able to prepare a system of two particles in an given state. He can generate this state of the two-particle system many times. Then, Charlie sends one particle to an observer, called Alice, while the other particle is transmitted to a different observer, Bob, situated at a distant location. Alice and Bob perform some measurements on their particles, and further the experiment is repeated many times.

Alice can measure any of two observables, denoted by $\mathcal{A}$ and $\mathcal{A}'$, associated to her particle. Suppose that the outcomes of the measurements, A and A', can each have only two values, namely 1 or -1. Alice chooses randomly which observable to measure for each particle of the pair.

Bob measures any of two observables associated to his particle, $\mathcal{B}$ and $\mathcal{B}'$, whose outcomes, denoted by B and B', can take the values 1 or -1. He chooses randomly which observable to measure each time he receives his particle of the pair. It is supposed that Alice and Bob perform simultaneously their measurements. We assume that a measurement of an observer cannot disturb the outcome of the other observer, situated in a different location.

Let us evaluate the following expression related to the outcomes A, A', B, and B':

$$AB + A'B + A'B' - AB' = (A + A')B + (A' - A)B'.$$

By using the fact that $A = \pm 1$ and $A' = \pm 1$, one obtains:

- $A + A' = 0$

  or

- $A' - A - 0$.

Therefore, the above expression can take only two values:

$$AB + A'B + A'B' - AB' = \pm 2.$$

Let us suppose, that, before the measurements performed by Alice and Bob, the two-particle system is found with the probability $p(a, a', b, b')$ in a state characterized by:

$$A = a,\ A' = a',\ B = b,\ B' = b'.$$

The following conditions must be fulfilled by $p(a, a', b, b')$:

$$\text{(i)}\ \ p(a, a', b, b') \in [0, 1],$$
$$\text{(ii)}\ \ \sum_{a,a',b,b'} p(a, a', b, b') = 1.$$

From the theory of probabilities, one knows that the mean value of AB is equal to:

$$E(AB) = \sum_{a,a',b,b'} p(a, a', b, b')\, a\, b.$$

Let us evaluate the mean value of the quantity $AB + A'B + A'B' - AB'$:

$$\begin{aligned} E(AB + A'B + A'B' - AB') &= \sum_{a,a',b,b'} p(a, a', b, b')\,(a\,b + a'\,b + a'\,b' - a\,b') \\ &\leq 2 \sum_{a,a',b,b'} p(a, a', b, b') = 2. \end{aligned} \tag{3.3}$$

On the other hand, we can compute the same expression in a different way:

$$\begin{aligned} E(AB + A'B + A'B' - AB') &= \sum_{a,a',b,b'} p(a, a', b, b')ab + \sum_{a,a',b,b'} p(a, a', b, b')a'b \\ &+ \sum_{a,a',b,b'} p(a, a', b, b')a'b' - \sum_{a,a',b,b'} p(a, a', b, b')ab' \\ &= E(AB) + E(A'B) + E(A'B') - E(AB'). \end{aligned} \tag{3.4}$$

From relations (3.3) and (3.4), we arrive at:

$$E(AB) + E(A'B) + E(A'B') - E(AB') \leq 2,$$

which is known in the scientific literature as the **CHSH-Bell inequality**, being proposed by the researchers Clauser, Horne, Shimony, and Holt. This is a generalization of an inequality initially discovered by John Bell.

Suppose that the state of the two particles prepared by Charlie is found in the singlet state:

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B).$$

Alice and Bob measures the spin of their particles along the directions $\vec{a}$, $\vec{a}'$, and $\vec{b}$, $\vec{b}'$, respectively. For some specific directions, the mean value computed using the quantum mechanics formalism leads to:

$$< AB > + < A'B > + < A'B' > - < AB' > = 2\sqrt{2},$$

which means that the CHSH-Bell inequality is violated. The experimental results confirm that the prediction of quantum mechanics is correct. This leads to the conclusion that the hypothesis of local realism proposed by EPR is wrong.

3.6 Quantum teleportation

3.6.1 The protocol of quantum teleportation

The protocol of quantum teleportation was proposed by Bennett *et al.* in 1993. The task is to transmit the information carried by a qubit held by Alice to another qubit held by Bob situated at a different location. The state of the qubit of Alice (denoted by 1) is found in an unknown state:

$$|\psi\rangle_1 = \alpha|0\rangle_1 + \beta|1\rangle_1, \tag{3.5}$$

where α and β are complex parameters, satisfying the normalization condition $|\alpha|^2 + |\beta|^2 = 1$.

Suppose that Charlie can prepare the Bell state $|\beta_{00}\rangle$ and he sends one particle, denoted by 2, to Alice, and the other particle, denoted by 3, to Bob as one can see in Fig. 3.2. The entangled two-qubit state $|\beta_{00}\rangle$ is called the quantum channel

$$|\beta_{00}\rangle_{23} = \frac{1}{\sqrt{2}}\left(|00\rangle_{23} + |11\rangle_{23}\right).$$

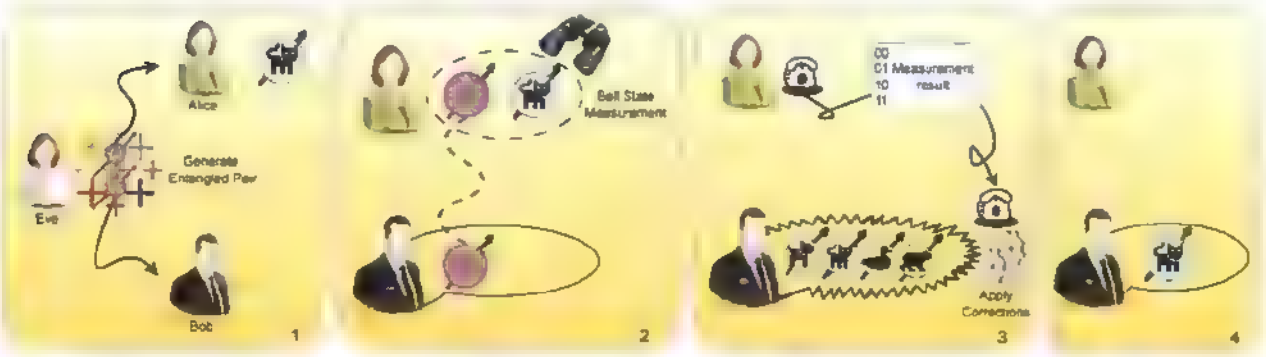


Fig. 3.2: The schematic diagram of quantum teleportation.

The state of the three-qubit system can be written as follows:

$$\begin{aligned} |\psi\rangle_1|\beta_{00}\rangle_{23} &= \frac{1}{\sqrt{2}}\left(\alpha|00\rangle_{12}|0\rangle_3 + \alpha|01\rangle_{12}|1\rangle_3 + \beta|10\rangle_{12}|0\rangle_3\right. \\ &\quad \left.+\beta|11\rangle_{12}|1\rangle_3\right). \end{aligned} \tag{3.6}$$

We obtain the two-qubit basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ in terms of the Bell states:

$$\begin{aligned} |00\rangle &= \frac{1}{\sqrt{2}}\left(|\beta_{00}\rangle + |\beta_{10}\rangle\right); \; |11\rangle = \frac{1}{\sqrt{2}}\left(|\beta_{00}\rangle - |\beta_{10}\rangle\right) \\ |01\rangle &= \frac{1}{\sqrt{2}}\left(|\beta_{01}\rangle + |\beta_{11}\rangle\right); \; |10\rangle = \frac{1}{\sqrt{2}}\left(|\beta_{01}\rangle - |\beta_{11}\rangle\right). \end{aligned}$$

We rewrite the three-qubit state as follows:

$$|\psi\rangle_1|\beta_{00}\rangle_{23} = \frac{1}{2}|\beta_{00}\rangle_{12}(\alpha|0\rangle + \beta|1\rangle)_3 + \frac{1}{2}|\beta_{10}\rangle_{12}(\alpha|0\rangle - \beta|1\rangle)_3 + \frac{1}{2}|\beta_{01}\rangle_{12}(\alpha|1\rangle + \beta|0\rangle)_3 + \frac{1}{2}|\beta_{11}\rangle_{12}(\alpha|1\rangle - \beta|0\rangle)_3. \quad (3.7)$$

Alice performs a Bell measurement (B. M.) of her particles 1 and 2 and then she communicates the output (classical communication) to Bob as one can see in Fig. 3.2. This is a partial measurement, since only particles 1 and 2 are involved (see Sec. 3.2 for details). Further, Bob applies a unitary operator U on the state of his qubit, depending on the outcome of the measurement of Alice. According to Equation (3.7), the Bob's unitary operator is as follows:

a) The state $|\beta_{00}\rangle$ is obtained with the probability 1/4. In this case, Bob has to do nothing, i.e. $U = I$, since the final state of his qubit is found in the desired state $\alpha|0\rangle + \beta|1\rangle$.

b) The state $|\beta_{10}\rangle$ is obtained with the probability 1/4, while the final state of particle 3 is $\alpha|0\rangle - \beta|1\rangle$. Further, Bob has to apply the Pauli operator Z and obtains the desired state.

c) The state $|\beta_{01}\rangle$ is obtained with the probability 1/4, while the final state of particle 3 is $\alpha|1\rangle + \beta|0\rangle$. Further, Bob has to apply the Pauli operator X and recovers the state.

d) The state $|\beta_{11}\rangle$ is obtained with the probability 1/4, while the final state of particle 3 is $\alpha|1\rangle - \beta|0\rangle$. Further, Bob has to apply the operator ZX and recovers the state.

We notice that in all the four cases, the state $\alpha|0\rangle + \beta|1\rangle$ is recovered, therefore the information of the qubit 1 was transmitted to the qubit 3 by using entanglement and classical comunication.

3.6.2 The quantum circuit of quantum teleportation

The purpose of this section is to present the quantum circuit of teleportation (see Fig. 3.3).

The input state is $|\xi_0\rangle = |\psi\rangle_1|\beta_{00}\rangle_{23}$, where the state $|\psi\rangle$ is given by Equation (3.5) and $|\beta_{00}\rangle$ is one of the Bell states. The particles 1 and 2 belong to Alice, while the particle 3 to Bob. The state $|\xi_0\rangle$ was computed in Equation (3.6).

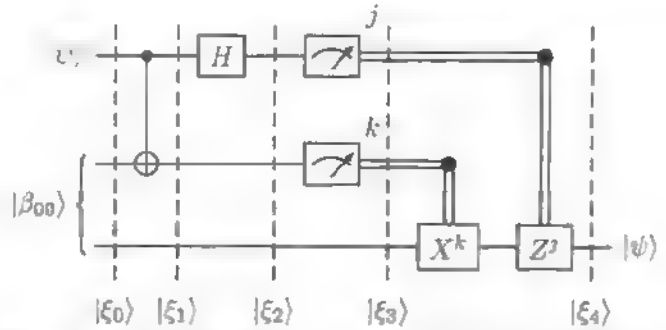


Fig. 3.3: The quantum circuit of teleportation.

Alice applies the CNOT gate on the states of particles 1 and 2 and obtains the state $|\xi_1\rangle$:

$$|\xi\rangle_1 = \frac{1}{\sqrt{2}}\left(\alpha|00\rangle_{12}|0\rangle_3 + \alpha|01\rangle_{12}|1\rangle_3 + \beta|11\rangle_{12}|0\rangle_3 + \beta|10\rangle_{12}|1\rangle_3\right).$$

The Hadamard gate applied on the state of particle 1 leads to:

$$\begin{aligned}|\xi_2\rangle &= \frac{1}{2}|00\rangle(\alpha|0\rangle + \beta|1\rangle) + \frac{1}{2}|10\rangle(\alpha|0\rangle - \beta|1\rangle) \\ &+\frac{1}{2}|01\rangle(\alpha|1\rangle + \beta|0\rangle) + \frac{1}{2}|11\rangle(\alpha|1\rangle - \beta|0\rangle).\end{aligned}$$

Alice performs a measurement of the particles 1 and 2 in the computational basis, generating the outputs $j = 0$ or 1 for particle 1, and $k = 0$ or 1 for particle 2 (see Fig. 3.3). The state of the particle 3 after the measurement, denoted by $|\xi_3\rangle$, depends on the Alice' outcome:

- 00: $|\xi_3\rangle = \alpha|0\rangle + \beta|1\rangle$;
- 10: $|\xi_3\rangle = \alpha|0\rangle - \beta|1\rangle$;
- 01: $|\xi_3\rangle = \alpha|1\rangle + \beta|0\rangle$;
- 11: $|\xi_3\rangle = \alpha|1\rangle - \beta|0\rangle$.

The last step of the quantum circuit requires the use of the quantum gate X^k, and further the quantum gate Z^j. In all the four cases (i) – (iv) described above, the final state of the particle 3 is the desired one:

$$|\xi_4\rangle = \alpha|0\rangle + \beta|1\rangle = |\psi\rangle,$$

i.e. the quantum teleportation is accomplished.

3.6.3 Milestones in quantum teleportation research

Two pioneering quantum teleportation experiments emerged in 1997 from separate research groups: one in Innsbruck, Austria, and another spanning Italy and the UK. D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, A. Zeilinger, in their Nature publication, demonstrated the teleportation of photon polarization. Meanwhile, D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu, in a Physical Review Letters article from 1998, explored teleportation of both linearly and elliptically polarized photons, managing to distinguish all four Bell states – a notable achievement of the era.

For an in-depth exploration of quantum teleportation's theory and experimental setups across varied systems, a comprehensive review was published by Pirandola *et al.* in Nature Photonics.

Chapter 4

Quantum Cryptography

In the previous chapters, two remarkable quantum communication protocols have been presented: the superdense coding algorithm and quantum teleportation. In this chapter we will rather explore the security perspectives for the reliable transmission of information by making use of basic quantum phenomena. This is the subject of the most spectacular applications of quantum information theory - quantum cryptography.

Specifically, cryptography is the science of secret and secure communication, which is aimed towards the protection of the private information from unauthorized access, and ensuring data integrity. In this regard, the usual practice is to apply a symmetrical (secret-key) cryptography represented in Fig 4.1, where Alice (the sender) is required to encrypt the message using a secret key, and to transmit it to Bob (the receiver), who decodes the message with a copy of the secret key, bewaring the interception of Eve (the eavesdropper). Such cryptosystems are the most computationally secure nowadays, thought it is essential for Alice and Bob to posses a common secret key. Yet, most widely used encryption schemes, such as RSA, involve the asymmetric cipher, commonly referred to as the public-key cryptography, which makes use of two different keys for the encryption and decryption.

However, classical cryptography relies solely on the hardness of certain mathematical problems, and therefore may prove to be insecure once tackled by sufficiently large quantum computers. Quantum cryptography, by contrast, is perfectly safe, enabling the communicating parties to detect if the transmitted message was compromised. This is achieved through the provably secure quantum key distribution (QKD) protocol, which solves the problem of secret key distribution in the symmetric cryptosystems by creating the private key bits between parties over a public quantum channel. Thus, any intrusion of Eve over the quantum channel in order to gain information about the state of the qubits disturbs the state of the quantum systems in such a way that it can be detected by the communicating parties. The resulting key can then be used to create a classical secure cryptosystem communication between Alice and Bob.

In the following we give a short overview over the vulnerabilities of classical protocols faced with quantum computing, and how we can leverage quantum phe-

nomena, namely entanglement, quantum uncertainty and no-cloning theorem, in order to achieve perfectly secure information transfer. Next, we elaborate on the QKD method and discuss different strategies for eavesdropping. In particular, we present three QKD protocols, along with their real-world applications: BB84, E91, and B92.

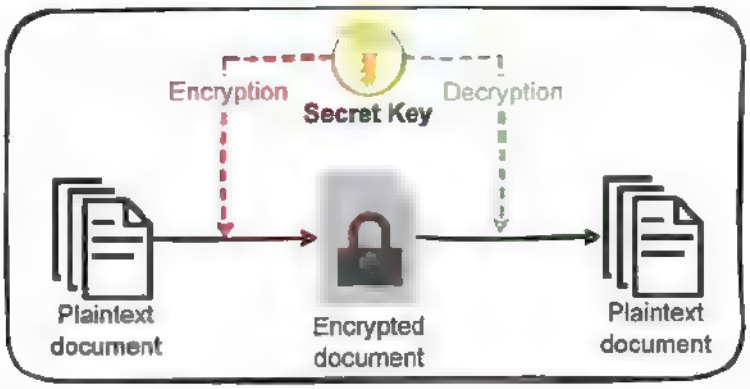


Fig. 4.1: The diagram of a symmetric encryption scheme.

4.1 The Quantum Gift: both threat and blessing

The traditional, widely-used, cryptographic protocols such as the RSA encryption protocol, Diffie-Hellman key exchange, or Elliptic Curve Cryptography, are vulnerable to attackers with sufficiently powerful quantum computers due to Shor's algorithm.

Shor's algorithm is a quantum algorithm developed in 1994 by Peter Shor, used for factorizing large integers. The ability to factorize large numbers is computationally intensive for classical computers, as the best algorithms have an exponential complexity. This difficulty underpins many classical encryption methods. Shor's algorithm, if a sufficiently large quantum computer is provided, can factorize integers in polylogarithmic time. Using the fastest multiplication algorithm known, Shor's algorithm needs an order of $\mathcal{O}((\log N)^2(\log\log N))$ quantum gates to compute the prime factors of an integer N.

Another quantum algorithm that poses a threat to classical cryptography is Grover's algorithm. Introduced in 1996 by Lov Grover, Grover's algorithm is designed to search an unsorted list, or solve black-box computational problems faster than classical methods. In a generalized way, to understand what this algorithm does, consider a function with a hidden property, and the goal is to find one input that produces a specific output. On a classical system, this search would take $\mathcal{O}(N)$ operations. Grover's algorithm can perform this search in $\mathcal{O}(\sqrt{N})$ operations, having a quadratic speedup over classical algorithms. In practice, this poses a threat against symmetric key cryptography (e.g. AES, DES). A brute-force classical search for an AES key would require 2^k operations, where k is the number of bits of the key.

With Grover's algorithm, this search would take only $2^{k/2}$ operations. Alongside protocols like AES, this algorithm could also potentially threaten applications that rely on cryptographic hash functions (e.g. digital signatures). However, unlike Shor's algorithm, mitigating the threat of Grover's algorithm can be as simple as doubling the length of the key, in order to restore the security level to the pre-quantum one.

Thus, quantum algorithms can pose a significant threat to classical cryptography, on the other hand however, we shall see in the following that through exploiting quantum phenomena like superposition, entanglement, and the no-cloning theorem, we can achieve perfect security of the quantum communication QKD protocols. We shall attempt to develop an intuition behind this statement in the following subsection.

4.1.1 Security guarantee by laws of physics

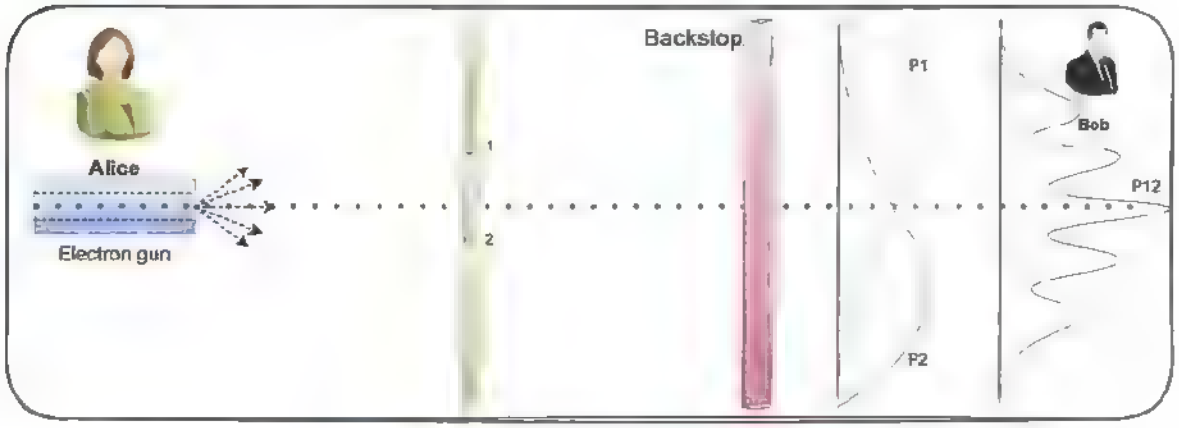


Fig. 4.2. Double slit experiment when electron trajectories are not observed.

The well-known double slit experiment can be regarded as an example of eavesdropping detection in the cryptographic communication protocols, as illustrated in Figs. 4.2 and 4.3. The sender, is a randomly emitting source of electrons that undergo a metal wall with two small slits. The backstop absorbing the electrons is used to identify the interference pattern described by the probability density P_{12}. We denote by P_1 the probability density when only slit 1 is open, and P_2 is the probability density for slit 2, respectively. The formalism of quantum mechanics explains this phenomenon by treating electrons as waves, such that $P_1 = |\varphi_1|^2$ and $P_2 = |\varphi_2|^2$, where φ_1 and φ_2 are probability amplitudes for the electrons passing through slits 1 and 2, respectively, while $P_{12} = |\varphi_1 + \varphi_2|^2$.

If we would want to know through which slit an individual electron passes through, we would need a way to observe the position of the electron. A common way to do this in the double slit experiment is with the help of a strong light source behind the wall, between the two slits. The light would scatter on the electron and thus we can observe its position. However, this process will destroy the interference pattern on the backstop so that the overall probability is given by the

sum of the probabilities of each alternative paths of the electrons, i.e. $P_{12} = P_1 + P_2$. This experiment is representative for any kind of quantum communication. If the interference pattern on the backstop, the receiver, aligns with this result, we can conclude that there is an eavesdropper on its quantum communication channel.

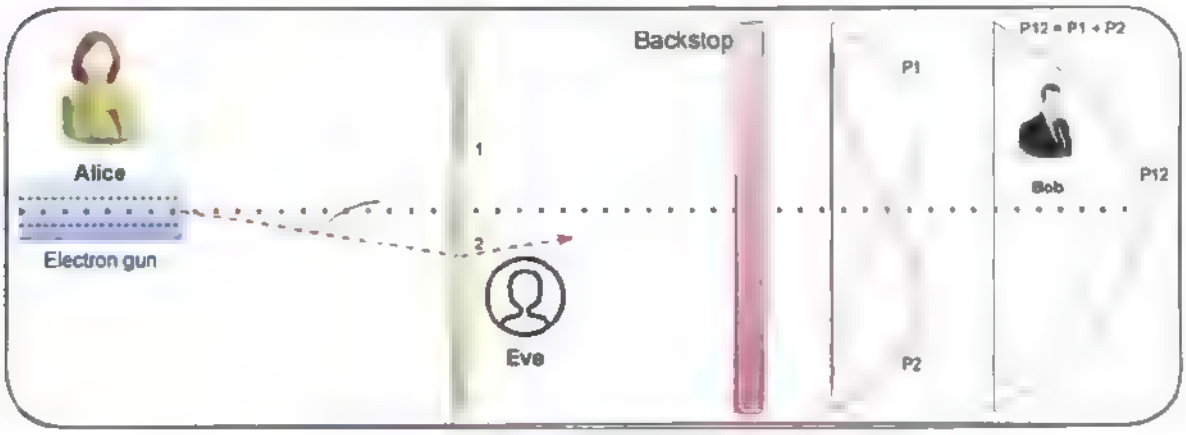


Fig. 4.3: Double slit experiment when electron trajectories are observed by Eve.

The quantum interference pattern is a result of a fundamental concept in quantum mechanics, namely the Heisenberg uncertainty principle. In this experiment, measuring the position of the electron x at the wall with precision Δx, you cannot, at the same time, know the momentum component received at the plate p more accurately than $\Delta p \geq h/2\Delta x$. Therefore, position and momentum are examples of two incompatible observables which cannot be both measured at the same time, and any attempt to learn something about one of the components will alter the measurements precision of the other.

The straightforward conclusion for the communication technologies is that the transmission of quantum information is protected by the fundamental laws of quantum mechanics. In the early 1970s, Stephen Wiesner was the first to notice the astonishing security advantage of quantum communications over classical protocols in his seminal paper. Though his early paper was rejected publication it was later published in 1983, and servers as the foundation of many modern quantum communication protocols, such as BB84 and B92.

4.2 QKD

Probably the best-known example of quantum communication is the QKD protocol that enables two communicating parties (Alice and Bob) to produce a shared secret key. The motivation of distributing keys securely, through quantum means, lies within the fact that we require unconditionally-secure communications. Through QKD, one may achieve this gold standard level of security by combining the keys generated with a cipher such as One Time Pad (OTP). While encryption protocols generally demand specific key sizes, OTP is especially notable for its extensive key

requirements. For OTP, keys must be as lengthy as the messages they encrypt, and there's a strict policy against key reuse, whether in entirety or partially. Although the integration of OTP with keys generated via Quantum Key Distribution (QKD) has been both theoretically explored and practically demonstrated in networks like SwissQuantum and Tokyo Metropolitan Network, its widespread use is curtailed in high-data-volume communications. This limitation primarily arises from the modest key generation rates of current commercial QKD hardware, which usually hover around 1-2 kilobits per second.

Achieving high-throughput key generation in QKD networks remains a challenging endeavor. Current QKD systems typically produce keys at a modest rate. For instance, the IDQ Cerberis XG QKD system delivers a rate of 1 Kb/s; Toshiba's Multiplexed QKD system manages 40 Kb/s, and Quintessence Labs' qOptica QKD system provides 4.3 Kb/s for distances exceeding 40km. To put this in perspective, even with a transfer rate of 50Kb/s, transmitting a single high-resolution 4Mb photograph would demand over a minute. This challenge intensifies when ensuring absolute security is paramount for end-user applications. Although QKD offers inherently secure keys, the task of enlarging these keys to meet application demands often necessitates Pseudo-Random Number Generators (PRNGs), compromising this unconditional security.

It should be noted that usually, the QKD procedure also relies upon a form of authentication, usually over a classical channel, of the two legitimate parties, as shown in Fig. 4.4. Authentication is needed to ensure that no man-in-the-middle attacks might happen, where a malicious eavesdropper might impersonate Alice to Bob, and Bob to Alice. Then, QKD involves encoding information in quantum states, or qubits, as opposed to classical communication's use of bits, and exploits certain properties of these quantum states to ensure its security.

Fig. 4.4: Schematic representation of the QKD protocol assisted with an authentited classical channel.

As a result of the QKD process, a key that is now only by Alice and Bob is established, as any third party that might have intercepted this key had to access the transmitted quantum states over the quantum channel would have been detected with a very high probability. Thus, the main advantage of QKD over traditional key distribution methods is that it relies upon foundations of quantum mechanics to ensure security, as opposed to the computational difficulty of finding the reverse mapping of a function. As such, QKD has provable security and provides forward secrecy.

4.2.1 Eavesdropping strategies

In the same way, a curious individual who tries to sneak a peek at a sensitive letter in a fragile envelope will likely leave signs of tampering, and so will an eavesdropper who tries to intercept quantum communications. An eavesdropper, Eve, in a classical scenario can perform an intercept-resend attack. This means that it intercepts a message, reads or stores it, and then forwards the original message to the destination. In such a situation, neither of the two legitimate communicating parties, Alice and Bob, can detect the eavesdropper.

In the case of eavesdroppers listening for quantum communications, this approach is faced with multiple problems. If Eve wants to store the quantum information and forward the original to Bob, this is forbidden by quantum mechanics: the no-cloning theorem (see Subsection 2.2.3). Also, as we have seen, quantum information is fragile, and it cannot be passively observed without altering it. Furthermore, a good strategy for secure communication is to encode a single bit of information into one of the two non-orthogonal quantum states randomly. This way Eve will not be able to distinguish between the two states of the qubits transmitted from Alice to Bob without disturbing their state.

Theorem. [Information gain implies disturbance][1] *Given that Alice sends to Bob one of the two non orthogonal states, $\psi_1\rangle$ and $\psi_2\rangle$, it is not possible to gain information, in any attempt to distinguish between them, without disturbing the state.*

Proof. 1. One process Eve may use to obtain information about which one of the quantum states was sent by Alice is to perform a measurement. A quantum state $|\psi_1\rangle$ can be measured without disturbing it if we measure an observable with the associated Hermitian operator for which $|\psi_1\rangle$ is an eigenstate. Moreover, in order to distinguish between $|\psi_1\rangle$ and $|\psi_2\rangle$, we require that both of them are eigenstates of the same Hermitian operator with two different eigenvalues, correspondingly. However, this is in contradiction with fact that $|\psi_1\rangle$ and $\psi_2\rangle$ are non-orthogonal states, and therefore, they cannot be eigenstates of the same operator and any measurement necessarily disturbs at least one of these states.

2. Another method Eve might apply in order to distinguish between the two states is to prepare an ancilla in a standard state $|u\rangle$ and let it to interact unitarily with the state ($|\psi_1\rangle$ or $\psi_2\rangle$) in such a way that the process does not disturb the states. Under this assumption one obtains the following:

$$\begin{aligned} U|\psi_1\rangle|u\rangle &= |\psi_1\rangle|v_1\rangle, \\ U|\psi_2\rangle|u\rangle &= |\psi_2\rangle|v_2\rangle, \end{aligned} \tag{4.1}$$

where $|v_1\rangle$ and $|v_2\rangle$ would have to be different so that Eve can acquire information about the state that was sent. However, unitary transformations preserve the inner products, such that

$$\begin{aligned} \langle v_1|\langle\psi_1|\psi_2\rangle|v_2\rangle &= \langle u|\langle\psi_1|U^\dagger U|\psi_2\rangle|u\rangle \\ &= \langle u|\langle\psi_1|\psi_2\rangle|u\rangle, \end{aligned} \tag{4.2}$$

and therefore, the following must hold

$$\langle v_1|v_2\rangle = \langle u|u\rangle = 1. \tag{4.3}$$

This means that $|v_1\rangle$ and $|v_2\rangle$ must be identical, and thus, Eve wont be able to distinguish between the two states.

□

Therefore, Alice and Bob will know if their link is compromised, and in that case they may choose to abort this procedure and re-start a new protocol, until they are assured, with high probability, that their key is private, and Eve is very limited in what she can do as an eavesdropper of quantum communications. In the following we proceed by describing three QKD protocols, the BB84, E91 and B92.

4.3 The BB84 protocol

Proposed in 1984 by Bennett and Brassard, BB84 is the first proper QKD scheme [11]. The protocol is based on the conjugate coding proposal of Wiesner [12], as it relies on the uncertainty principle and the no-cloning theorem to achieve security.

Specifically, the BB84 protocol requires Alice to generate two classical random n-bit sequences k and a, and to encode each element k_i in a qubit with a quantum state $|v\rangle$ in the X basis $\{|0\rangle, |1\rangle\}$, or Z basis $\{|+\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$ (see Equation 1.3), depending on a_i, as follows:

$$\begin{cases} 0 \longrightarrow |0\rangle, & 1 \longrightarrow |1\rangle, \quad \text{for} \quad a_i = 0. \\ 0 \longrightarrow |+\rangle, & 1 \longrightarrow |-\rangle, \quad \text{for} \quad a_i = 1. \end{cases}$$

Alice then sends $|v\rangle$ to Bob, over a public and classically-authenticated quantum communication channel, meaning that Alice and Bob first need to send an authentication key over a classical secure channel, and then they implement the BB84 quantum protocol and "expand" the existing authentication key.

After Bob receives $|v\rangle$ he will choose at random between X and Z basis to measure each qubit in, according to a random $n-$bit vector b. Finally, both Alice and Bob, announce their n-bit strings (i.e. a and b) on the public channel, and the shared key $\tilde{k}$ is composed of the bits k_i where $a_i = b_i$. An example of key distribution using BB84 protocol with 10 qubits is shown in Figure 4.5. On average, Bob will choose the same basis as Alice half the time, and thus, the length of the key will be roughly equal to:

$$|\tilde{k}| \approx \frac{|k|}{2} = \frac{n}{2}.$$

4.3.1 Eavesdropper scenario

As the classical channel is authenticated, Eve has the possibility to reliably perform just one attack: intercept-resend. As she has no information regarding

k	0	0	1	1	0	1	0	1	0	0
a	1	0	1	0	1	0	1	0	1	1
A sends	$\|+\rangle$	$\|0\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|+\rangle$
b	1	1	0	1	1	0	0	0	0	1
B measures	$\|+\rangle$	$\|+\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|+\rangle$
Bases	✓	✗	✗	✗	✓	✓	✗	✓	✗	✓
$\tilde{k}$	0				0	1		1		0

/Fig. 1.5: Example of BB84 protocol with $n = 10$ qubits.

what basis Alice used to prepare it) when she intercepts the qubits, and she cannot store the qubits, or copies of them (the no-cloning theorem), she can only pick random basis for measurement (a sequence e of n bits).

Note that the states in the X basis are not orthogonal to the states in the Z basis (see Subsection 1.3.1), and therefore, there is no measurement that an intercepting Eve can perform, in order to distinguish between them with certainty (see the Information Gain theorem stated above). Also, spin Pauli operators X and Z are incompatible operators, and due to Heisenberg uncertainty principle measuring one of them will destroy the previous determination of the spin in the other direction. For each qubit, there are several possibilities for the outcomes of the measurements for each basis choice of Eve, which is shown in Figure 4.6.

Eve's basis	Bob's basis	Eavesdropping detection
$\bar{e}_i = a_i \rightarrow$ qubit altered (no information gain)	$a_i = b_i$	50% pr. to be detected
	$a_i = \bar{b}_i$	bit discarded
$e_i = a_i \rightarrow$ qubit unaltered (information gain)	$a_i = b_i$	undetected
	$a_i = \bar{b}_i$	bit discarded

Fig. 4.6: Possible outcomes for Eve when eavesdropping on the quantum channel of BB84.

As we can see, out of four equally probable scenarios just in one case Eve goes undetected while also gaining information, and that is when she and Bob as well, guess the right basis, i.e. the basis that Alice encoded the information in. In other two cases, either Eve chooses the right basis of Alice or not, however if Bob chooses the wrong basis then the results of this measurements are discarded once Alice and Bob publicly announce their bases.

One last possible scenarios is when Eve wrongly guesses the basis of Alice, and therefore, Eve gains no information and Bob receives an altered qubit. However, there is 50% probability that after Bob performs his measurement it will result in a bit error in the key. In order to ensure that no tampering by a malicious third party has occurred, Alice and Bob can deploy simple strategies from classical cryptography, namely, they can perform information reconciliation and privacy amplification to distill a shared secret key string. For instance, information reconciliation is a classical

error correction protocol aver a public transmission channel. where the two parties compare subsets of their keys. If no tampering occurred and no noise affected $|\psi\rangle$ over the quantum channel. the subset k_A of Alice will match the subset k_B of Bob. If these subsets do not match. they will be able to detect the error caused by tampering or noise.

This means that Eve has 75% change of reading the qubit undetected, but only 25% of getting useful information. However. since Eve would need the entire key to be able to decrypt any subsequent sensitive information sent between Alice and Bob, Eve would need to read all n qubits undetected. This probability is dictated by the equation $p_e = \left(\frac{3}{4}\right)^n$

For example, if Alice and Bob exchange 48 qubits per key. Eve would have an almost one in a million chance of reading this key undetected.

If Eve gets detected. through the process discussed previously. Alice and Bob will abort and start the procedure again. It is important to note that the quantum channels are inherently noisy, and the two subsets of bits compared by Alice and Bob will not perfectly match. As such. they will use a threshold. and if the mismatches are above that threshold they will restart the procedure. Therefore there is. a very unlikely possibility. that Eve gets very lucky and is able to pick all the correct bases and still get undetected.

4.4 The E91 protocol

E91 is a QKD scheme proposed by Artur Ekert in 1991 that uses entangled pairs of photons [13], distributed in a way such that Alice and Bob share one of the Bell states defined in Equation (3.3). It is one of the foundational QKD protocols. alongside BB84.

The first step of this distribution scheme is generating the entangled pairs. The source can be either Alice or Bob. but can also be a third party. Alice and Bob must each receive one photon of the entangled pair.

Following the entangled pair distribution. both Alice and Bob must randomly choose one of several measurement bases to measure their respective photons. The choices are designed such that they can be used to test the violation of a Bell inequality (see Section 3.5). Alice and Bob will independently measure their photons using the basis they've chosen. It is crucial that they keep the bases they have chosen secret until measurements have been completed.

After the measurement. Alice and Bob can publicly announce which bases they have used. without revealing the actual outcomes. They will discard the results of the instances where they did not use matching bases. similar to the BB84 protocol.

In order to test for tampering. they will test for a Bell Inequality violation. using a subset of their shared results. If the inequality is violated. as expected for entangled particles. it indicates that there was no tampering of the entangled pairs. In case the inequality is not violated. key generation is restarted. If the subset of entangled pairs passes the Bell Inequality test. the subset is used to generate the

shared secret key.

Compared to BB84, E91 provides an inherent mechanism of testing for eavesdroppers. This test is enforced by the entangled properties of the particles used, as opposed to a statistical method used in BB84.

4.5 The B92 protocol

In 1992, Charles Bennett proposed a new protocol for QKD, this time using only two non-orthogonal states [14]. In essence, B92 is a modified version of the BB84 protocol, that only uses two polarization states. As stated, the main departure from BB84 is the fact that the encoding uses only two non orthogonal quantum states. These can be any two non-orthogonal quantum states.

Since the two states are non-orthogonal, they cannot be perfectly distinguished from each other using a single measurement (see the Information Gain theorem stated above). Thus, the preparation and transmission stage will need to be performed multiple times by Alice. Note, however, that Bob will retain the bases he chose initially, for every measurement.

Bob will measure the incoming qubits of the sequence randomly in one of two bases. The bases in which Bob measures are chosen in a way to maximize his chance of measuring one of the two non-orthogonal states that Alice encoded. Since the states are non-orthogonal, there is no one basis that can serve this purpose. For example, Alice may use the following encoding scheme:

$$|\psi\rangle = \begin{cases} |0\rangle, & \text{for} \quad a_i = 0, \\ \frac{|0\rangle+|1\rangle}{\sqrt{2}}, & \text{for} \quad a_i = 1. \end{cases}$$

Bob performs measurements randomly, in basis $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$, as defined in Subsection 1.3.1. If he projects the qubit on the state vector $|+\rangle$ and obtains $|1\rangle$ then he concludes that $a_i = 1$, otherwise, if he obtains $|0\rangle$ then the measurement is not conclusive. Similarly, if Bob uses the X basis and obtains $|+\rangle$, then the initial state could have been $|0\rangle$ or $|+\rangle$, however if he obtains $|-\rangle$ then the initial state could be only $|0\rangle$. Therefore, when Bob gets a conclusive measurement result of a qubit, it means that he measured the qubit on the "correct" basis, matching Alice's preparation.

Alice and Bob will then communicate over a public channel, where Bob announces which qubits gave conclusive results, but not the actual results. Alice and Bob will then know which qubits were successfully transmitted and measured, and they form their shared secret key from these qubits.

The mechanism to detect eavesdroppers is similar to the one used in BB84. While the B92 protocol is more streamlined than BB84, it typically requires a higher qubit transmission rate for the same key distribution rate, due to how many qubits will be discarded by Bob.

4.6 Real-world application and technologies

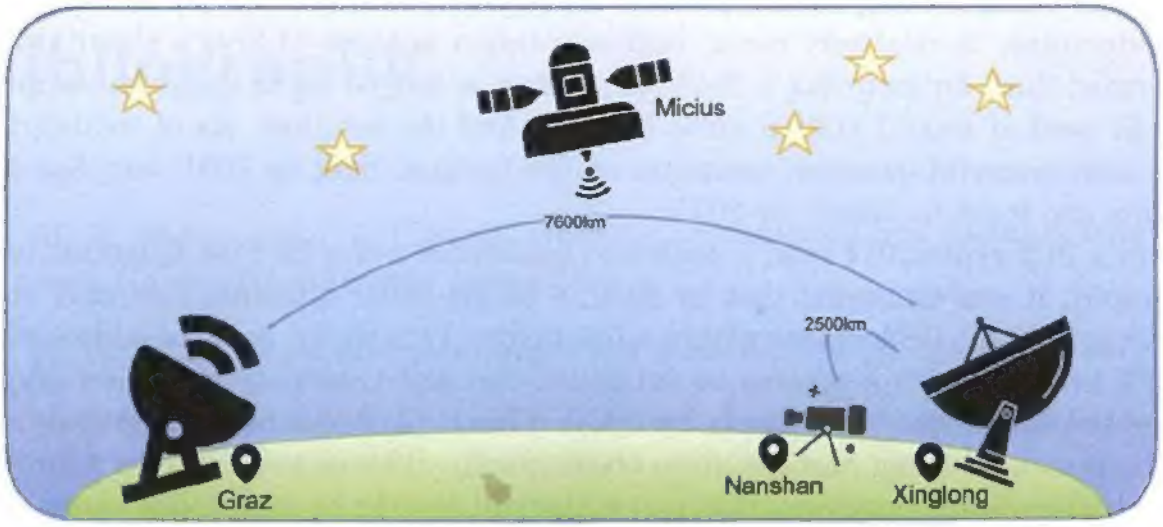


Fig. 4.7: Long distance QKD using Micius satellite[15].

A way to use these secure keys in order to transmit data is to use them in conjunction with a symmetric cipher. One such cipher is a one-time pad (OTP). The OTP algorithm is known for its impeccable security profile when implemented correctly. Each bit or character from the plaintext is encrypted by a modular addition with a bit or character from a secret random key or 'pad' of the same length. This results in the ciphertext, which is then sent over an insecure channel. The receiver, possessing an identical copy of the key, can reverse the process and decrypt the message. Given the keys are truly random, as long as the plaintext, is used only once, and kept completely secret, the OTP is unbreakable, providing perfect secrecy.

Regarding real-world achievements, in 1989 Bennett and Brassard performed the first QKD experiment over a distance of 32cm between the nodes. This marked the first stepping stone in establishing large distance-spanning QKD networks. In 2006 a European collaboration led by Ursin et al., QKD over a FSO medium between two of the Canary Islands situated 144km apart was achieved.

In 2007, a collaboration between NIST and Los Alamos National Laboratory achieved QKD over 148.7km of optic fiber by Hiskett et al in 2006. The significance of this realization is that the vast majority spans of optic fiber in current classical networks are shorter than this distance.

In September 2017, the first quantum "video call" was performed between Beijing, China, and Vienna, Austria, using QKD to secure the transfer of data by Liao et al. The QKD was facilitated by the Chinese satellite Micius, the total distance of the transmission being up to 1200km.

Most of these scientific realizations used foundational QKD schemes, that have been theorized in the 1980s, or early 1990s.

4.7 Post-Quantum Cryptography

Through all previously discussed threads and guarantees that the quantum paradigm offers the realm of information security, it is clear that great changes are imminent. The only thing holding back the tide is the physical limitations of current quantum architectures. A relatively recent implementation analysis of Shor's algorithm determined that, for factoring a 2048-bit number, a 400000 qubit quantum computer would need at least 1 trillion qubit-hours to find the solution. As of writing this, the most powerful quantum computer on the horizon, built by IBM, only has 4000 qubits and is set to launch by 2025.

In a PQCrypto 2014 talk, a dedicated conference series for Post Quantum cryptography, it was estimated that by 2030, a billion-dollar quantum computer could break a 2000-bit RSA cipher within a few hours. This threat is being addressed by NIST head-on, with a process to determine the best candidate for a new cryptographic system, due to be ready by 2024. This is part of a more large-scale shift towards standardizing post-quantum cryptography. This movement aims to provide quantum-resistant protocols, that can withstand attacks by malevolent actors with access to powerful quantum computers.

4.7.1 NIST standardization

The NIST standardization initiative for post-quantum cryptography has been ongoing since 2016. The process was initiated with the call for proposals stage, inviting researchers worldwide to submit candidate algorithms for post-quantum cryptographic standards. These proposals included encryption algorithms, key distribution algorithms, and digital signature algorithms. After the deadline, one year later, 82 submissions were received, and by July 2020, 7 "finalists" and 8 "alternates" remained. The evaluation process consisted of 3 phases, which involved rigorous cryptanalysis and performance evaluation to identify any potential vulnerabilities or inefficiencies.

There are multiple types of post-quantum algorithms proposed, based on the mathematical structures they rely upon. Among those submitted, there were 26 lattice-based algorithms, 19 code-based algorithms, 9 multivariate polynomials-based, 3 symmetric cryptography-based, and a few other categories for digital signatures.

In 2022, NIST presented four post-quantum cryptography candidates for standardization. By August 2023, three drafts were open for public comments. It is noteworthy that NIST envisions a transitional phase, combining classical and post-quantum systems, ensuring security as the latter gains adoption across the industry.

Bibliography

[1] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*. Cambridge university press, 2010.

[2] A. Peres, *Quantum theory: concepts and methods*, vol. 72. Springer, 1997.

[3] N. S. Yanofsky and M. A. Mannucci, *Quantum computing for computer scientists*. Cambridge University Press, 2008.

[4] G. P. Popescu, Z.-M. Mina, and A. Tănăsescu, *Lecture notes in Quantum Computing*. Computer Science and Engineering Department, University Politehnica of Bucharest, 2017-2023.

[5] G. P. Popescu and O. Stănăşilă, *Provocările Calculului Cuantic*. Politehnica university press, 2019.

[6] R. P. Feynman *et al.*, "Simulating physics with computers," *Int. J. Theor. Phys*, vol. 21, no. 6/7, 1982.

[7] Y. Manin, "Computable and uncomputable," *Sovetskoye Radio, Moscow*, vol. 128, p. 28, 1980.

[8] P. Benioff, "The computer as a physical system: A microscopic quantum mechanical hamiltonian model of computers as represented by turing machines," *Journal of statistical physics*, vol. 22, pp. 563–591, 1980.

[9] D. Deutsch, "Quantum theory, the church–turing principle and the universal quantum computer," *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, vol. 400, no. 1818, pp. 97–117, 1985.

[10] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.

[11] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, pp. 7–11, 2014. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[12] S. Wiesner, "Conjugate coding," *SIGACT News*, vol. 15, p. 78–88, jan 1983.

[13] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661–663, Aug 1991.

[14] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, pp. 3121–3124, May 1992.

[15] S.-K. e. a. Liao, "Satellite-relayed intercontinental quantum network," *Phys. Rev. Lett.*, vol. 120, p. 030501, Jan 2018.